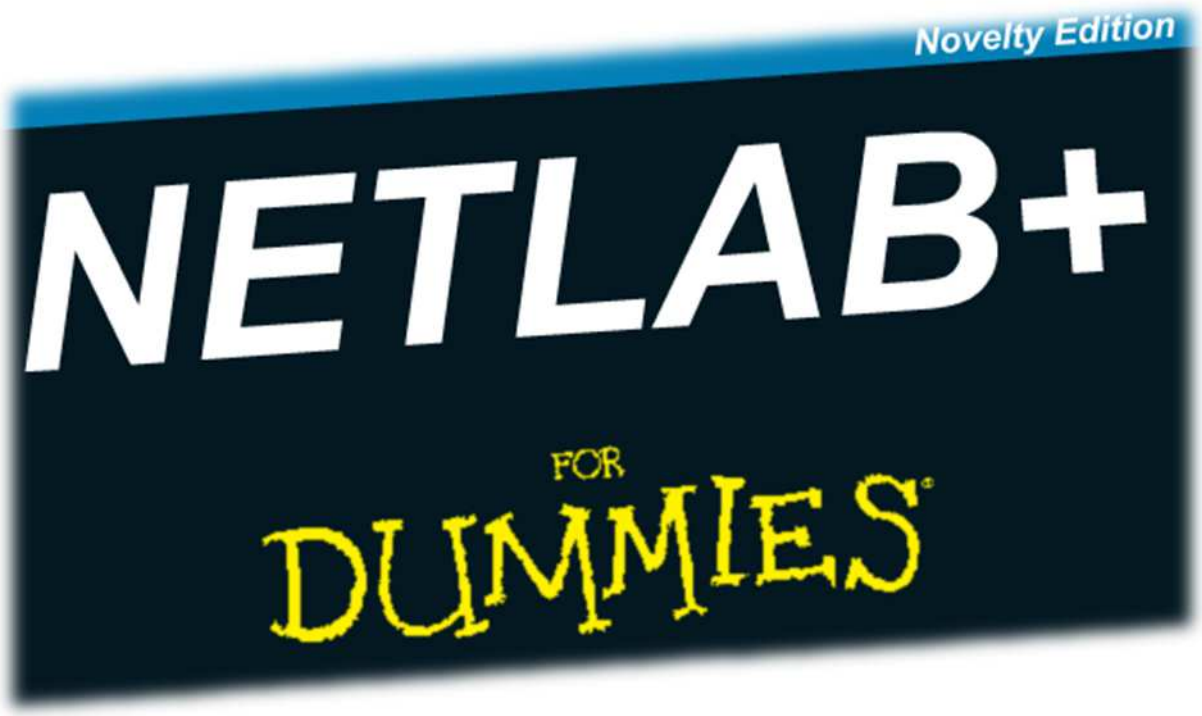



*June 2014*

*Version 1.00*

*This guide will help lead the process of installing and configuring a NETLAB+ server appliance. It will also include the ideas of VMware ESXi and vCenter virtualization products along with Cisco equipment used for Cisco specific pods.*

NETLAB+ Academy Edition, NETLAB+ Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc.

# Table of Contents


1 Introduction ..... 5

*1.1 ....What is NETLAB+* ..... *5*

*1.2 ....What Can NETLAB+ Deliver* ..... *5*

*1.3 ....Requirements* ..... *5*

1.3.1 Core Topology ..... 6

1. NDG NETLAB+ Server ..... 6

1.3.2 Optional Live Equipment ..... 7

*1.4 ....Planning Ahead with VMware* ..... *8*

1.4.1 VMware Version Comparison ..... 8

1.4.2 Obtaining VMware Licenses ..... 9

*1.5 ....Network Models* ..... *9*

1.5.1 Single-Homed Networking ..... 10

1.5.2 Dual-Homed Networking ..... 12

*1.6 ....Connectivity* ..... *13*

1.6.1 Internet Connection ..... 13

1.6.2 Network Address Translation (NAT) ..... 14

1.6.3 Outside to Inside Firewall Requirements ..... 14

1.6.4 Inside to Outside Firewall Requirements ..... 14

2 Installing the NETLAB+ Server Appliance ..... 15

*2.1 ....Background* ..... *15*

*2.2 ....Connect NETLAB+ to Outside Network* ..... *15*

*2.3 ....How to Access the NETLAB+ Console* ..... *15*

*2.4 ....Connect to a Power Source* ..... *15*

*2.5 ....Accessing the Console* ..... *15*

*2.6 ....NETLAB+ IP Configuration* ..... *16*

*2.7 ....Outbound Firewall Test* ..... *18*

*2.8 ....Connecting to the NETLAB+ Web-Based Interface* ..... *19*

*2.9 ....Logging into NETLAB+ as an Administrator* ..... *19*

*2.10 ..Remote Access Test* ..... *19*

*2.11 ..Check for Software Updates* ..... *20*

*2.12 ..Configure NETLAB+ Services* ..... *20*

*2.13..NETLAB+ Maintenance Reminder....21*
3 Configuring BIOS and RAID Configuration ....22
*3.1 ....Background ....22*
*3.2 ....BIOS Changes ....22*
*3.3 ....RAID Configuration ....25*
3.3.1RAID Configuration Utility - 8x2TB HDD using RAID 5 ....26
4 VMware ESXi Server Setup ....31
*4.1 ....Background ....31*
*4.2 ....Preparing the ESXi Server ....31*
*4.3 ....Installing the ESXi Server ....31*
*4.4 ....Basic Network Configuration ....33*
*4.5 ....Request for NDG Optimized vCenter Server Appliance....35*
*4.6 ....Installing the vSphere Client....35*
*4.7 ....Deploying vCenter Server Appliance....37*
*4.8 ....Configuring Network Settings....40*
*4.9 ....Creating a NETLAB+ User on the vCenter Appliance....43*
*4.10..vCenter Appliance Initial Configuration....44*
*4.11..Setting Hostname and Changing the root Password....45*
*4.12..Automatic Startup for vCenter....47*
*4.13..Datacenter Configuration....48*
4.13.1 Creating NETLAB+ Datacenter in vCenter ....49
4.13.2 Creating a NETLAB+ Role in vCenter....50
4.13.3 Adding ESXi Hosts to the NETLAB+ Datacenter ....53
4.13.4 Configuring ESXi Firewall to Allow Remote PC Viewer Sessions....55
*4.14..vSwitch Configuration....56*
*4.15..Verifying vSwitch0 Configuration ....57*
*4.16..Inside Network Configuration....58*
4.16.1 Creating vSwitch1 and Binding to a Physical NIC....59
4.16.2 Increasing the Inside vSwitch Port Count....61
4.16.3 Creating a SAFETY NET....64
5 Configuring NETLAB+ ....66
*5.1 ....Background ....66*

*5.2 ....Register a Virtual Datacenter with NETLAB+* ..... 66
*5.3 ....Adding ESXi Host(s) in NETLAB+* ..... 67
*5.4 ....Proactive Resource Awareness* ..... 69
*5.5 ....Local System ID for Multiple NETLAB+ Systems* ..... 72
6 Administrator Guide ..... 73
*6.1 ....Background* ..... 73
*6.2 ....Editing the Administrator Profile* ..... 73
*6.3 ....Managing Communities* ..... 74
6.3.1 Adding Communities ..... 74
*6.4 ....Managing Classes* ..... 76
6.4.1 Adding Classes ..... 76
6.4.2 Adding Learners to the Class Roster ..... 78
6.4.3 Adding Lead Instructors to a Class ..... 80
*6.5 ....Managing Accounts* ..... 80
6.5.1 Adding Accounts ..... 81
6.5.2 Modifying Instructor Privileges ..... 82
*6.6 ....Managing Global Lab Authorization Options* ..... 83
*6.7 ....Equipment Pods* ..... 85
6.7.1 Adding Pods ..... 85
6.7.2 Adding Custom Pods ..... 85
7 Lab Reservations ..... 86
*7.1 ....Scheduling a Lab Session as a Student* ..... 86
*7.2 ....Changing Lab Exercises* ..... 89
8 Best Practices ..... 90
*8.1 ....Background* ..... 90
*8.2 ....Normal vs. Persistent VMs* ..... 90
8.2.1 Normal ..... 90
8.2.2 Persistent ..... 91
*8.3 ....Breakdown of Proper Pod Creation & Cloning* ..... 91
8.3.1 Importing VMs into the Virtual Machine Inventory ..... 91
8.3.2 Creating a Master Pod ..... 93
8.3.3 Link Cloning a Master Pod ..... 97
9 References ..... 100

# 1 Introduction

## 1.1 What is NETLAB+

NETLAB+ is an internet based virtual lab provider for instructor led training developed by Network Development Group, Inc. NETLAB+ helps provide students with live interactive equipment that is physically placed within a datacenter. This specialized software has a calendar interface, which allows learners to reserve access to the live equipment. This allows for individual students or teams to schedule equipment use in a selected time frame. All a student really needs is a stable internet connection to connect to NETLAB+.

NETLAB+ provides a safe "sandbox" feature for users to schedule, configure, and interact with lab equipment. All supporting devices are located behind the NETLAB+ server and not directly exposed to outside public networks.

For the admin's perspective, the NETLAB+ system server that is incorporated into your datacenter requires no customer knowledge of UNIX, web server software, or other specialized system administrator functions. NETLAB+ comes already preconfigured with the loaded software.

## 1.2 What Can NETLAB+ Deliver

NETLAB+ delivers real-time access to the equipment in a training environment which allows students and instructors to simultaneously share connections to the same equipment. With the support of instructor-led class lectures, instructor self-preparation, student teams, and student self-study, NETLAB+ is a gateway to real lab time without the hassle of spending time to set up labs like you normally would in a physical classroom.

With the help of automation, instructors can now focus on teaching. NETLAB+ provides easy management by adopting manual tasks and simplifying them with loading and saving device configurations, recovering lost passwords, scrubbing equipment, and preparing the equipment for the next reservation. NETLAB+ also helps reduce energy costs by powering off equipment when no upcoming reservations are scheduled.

Implementing a NETLAB+ system can offer many training benefits such as making distance learning possible, fully utilizing equipment and sharing resources, increasing student lab time, potential to access equipment at other schools, hosting academy curriculum, and an easy-to-use graphical user interface (GUI) for system administrators.

## 1.3 Requirements

NETLAB+ requires essential core components to fully operate. Along with the core components, optional components may be discussed if you plan on supporting real lab equipment such as Cisco Networking Academy content. All of this will be discussed in the following section.

### 1.3.1 Core Topology

The following diagram displays the major components that make up a typical NETLAB+ system setup using *VMware vCenter* and *VMware ESXi 5.1*.

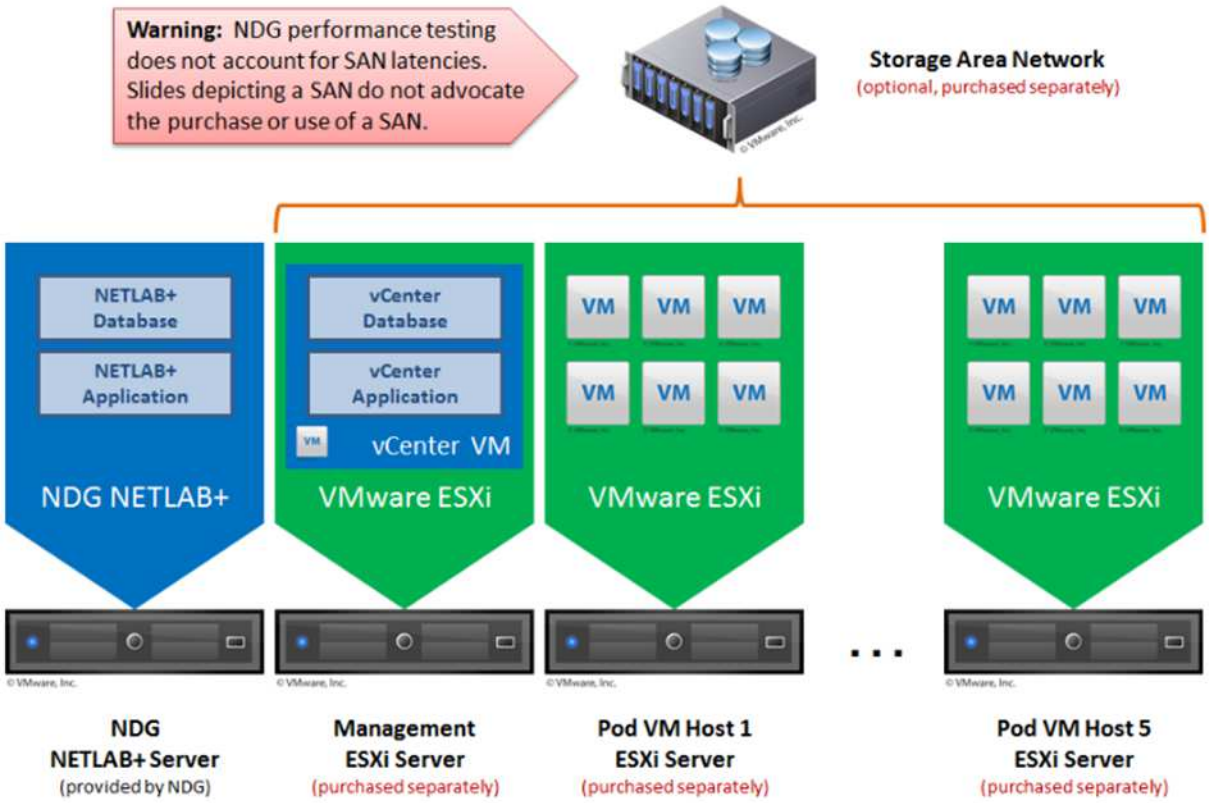



Diagram from Remote PC Guide Series – Volume 1 NetDevGroup.com

1. **NDG NETLAB+ Server**

   The NETLAB+ server provides the user interface for student and instructor access. The same interface but for administrators is used to manage VMs and software features to automate virtual machine pod creation.

   The NETLAB+ appliance comes in two different software licenses, NETLAB+ Academy Edition (AE) and NETLAB+ Professional Edition (PE). More information can be found in the following link: http://goo.gl/RoHxTw

2. **Management ESXi Server**

   The management server will be a server that is running on ESXi . It will host a virtualized *VMware vCenter Appliance* which is used to manage your physical ESXi host servers. NETLAB+ communicates with the *vCenter* to perform automated tasks and virtual machine management.

NDG has provided a recommended specification table that outlines what model and hardware have been marked compatible with NETLAB+. More information can be found at the following link: http://goo.gl/DbJKty

3. **Physical Host ESXi Server**

   The physical ESXi servers host the virtual machines in your virtual machine pods. NDG has provided a recommended specification table that outlines what model and hardware have been marked compatible with NETLAB+. More information can be found at the following link: http://goo.gl/DbJKty

### 1.3.2 Optional Live Equipment

If you decide to host live equipment for the Cisco Networking Academy content, you will then expand beyond the core topology and include devices such as access servers, control switches, and switched outlets. These devices are considered to be "control devices" and are needed to support access to the individual Cisco pods.

To find out more information about what control devices are supported by NETLAB+, please visit the following link: http://goo.gl/yP3keW

When building Cisco pods, you will need to acquire additional equipment that will be used as "lab devices" which students will actually be accessing and configuring. NDG is constantly updating their supported lab device list. If you wish to find out more information as to what lab devices are fully supported by NETLAB+, please visit the following link: http://goo.gl/YLR0yu

The following diagram shows a topology that includes Cisco equipment:

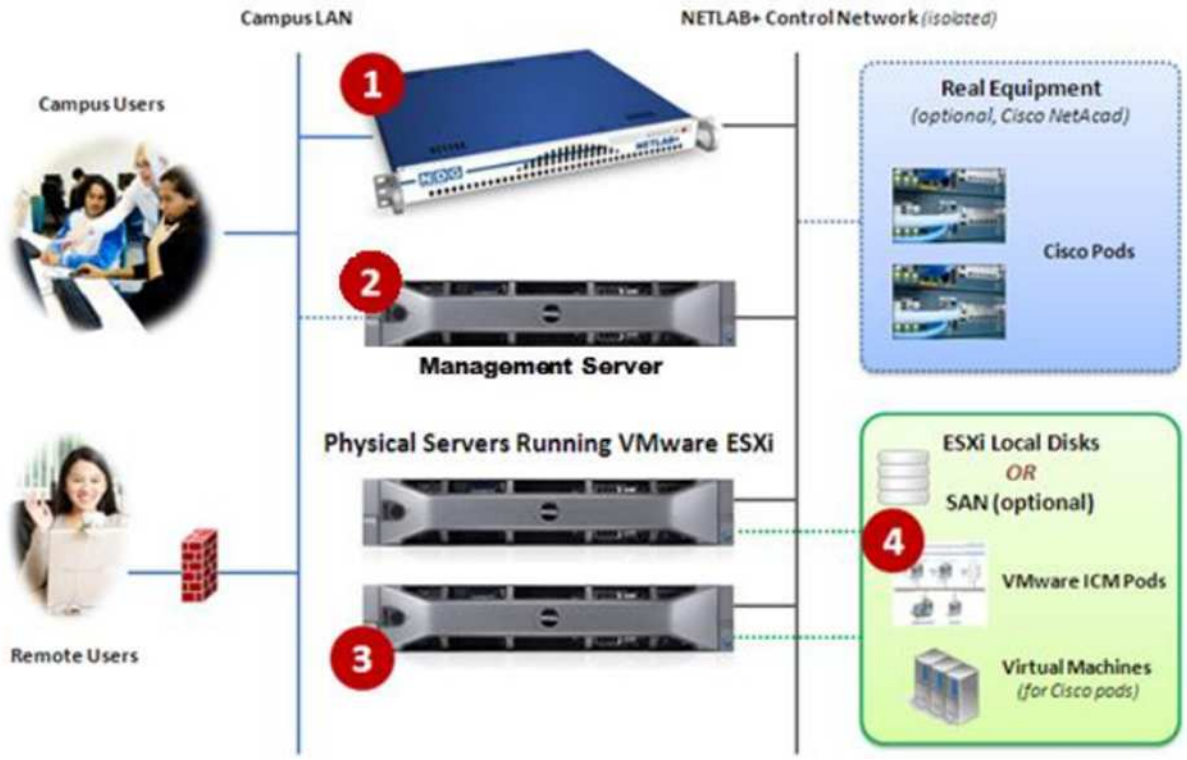



Diagram from Remote PC Guide Series – Volume 1 NetDevGroup.com

## 1.4 Planning Ahead with VMware

At this phase, you will want to make a checklist of all the hardware that you will need to suit your curriculum requirements. How many different courses are you teaching that will use NETLAB+? How many students will be registered in each course?

### 1.4.1 VMware Version Comparison

When planning to build your infrastructure to support NETLAB+, it is crucial to pick a VMware version that is supported by NDG. The following table compares VMware ESXi versions for hosting products.

| VMware Product | VMware ESXi vCenter | VMware ESXi vCenter | VMware ESXi vCenter | VMware ESXi Standalone |
|---|---|---|---|---|
| VMware Major Version(s) | **5.1** | **4.1 U2** | **4.01** | **4.01** |
| NETLAB+ Support | **Recommended** | Supported | Deprecated | Deprecated |
| Minimum NETLAB+ Version | 2011.R2 | 2011.R2 | 2011.R2 | 2009.R1 |
| Architecture | Bare Metal Hypervisor | Bare Metal Hypervisor | Bare Metal Hypervisor | Bare Metal Hypervisor |
| VMware Versions Tested by NDG | 5.1 | 4.1 U2 | 4.01 | 4.01 |
| Host Operating System Required | No | No | No | No |
| vCenter Required | **Yes** | **Yes** | **Yes** | No |
| Support ICM 4.1 Pods | **Yes** | **Yes** | **No** | No |
| Support ICM 5.0 Pods | **Yes** | **Yes** | **No** | No |
| Support ICM 5.1 Pods | **Yes** | **Yes** | **No** | No |

Diagram from Remote PC Guide Series – Volume 1 NetDevGroup.com

### 1.4.2 Obtaining VMware Licenses

You may acquire VMware license keys either through the VMware IT Academy Program (vITA) or by the VMware Academic Program (VMAP). License keys are required, as without them, your *vCenter* and ESXi infrastructure will not operate to its potential.

Since licensing conditions may vary depending on your school's participation, a VMware Product Licensing chart has been provided by NDG.

## 1.5 Network Models

NDG likes to illustrate two different network models based on the school's curriculum. Two different network models are mentioned.

- Single-Homed Networking
- Dual-Homed Networking

### 1.5.1 Single-Homed Networking

A Single-Homed network model is used when you are only hosting virtual machines and not live equipment such as Cisco devices. This model connects one NIC from each server to a routable network on your campus. All traffic flows across the campus LAN.

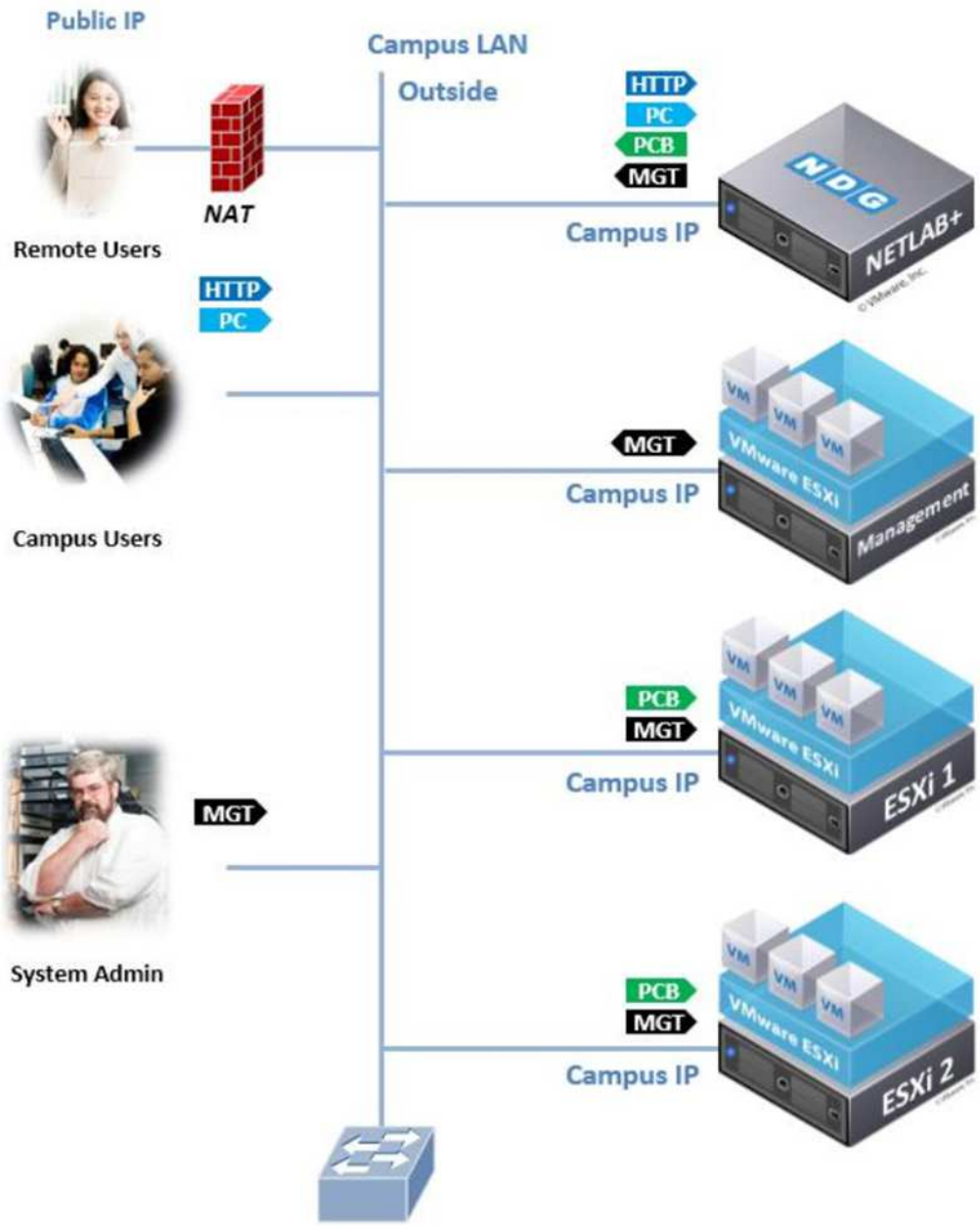



Diagram from Remote PC Guide Series – Volume 1 NetDevGroup.com

When using this model, you are not required to have NETLAB+ control switches. A minimum 1Gb/sec switch port is highly recommended for each server connection to the campus LAN.

When allocating space for your Single-Homed network model, the following tasks need to be revised:

- First, obtain an IP address, subnet mask, and default gateway for each outside server interface connected to the LAN.
- Connect the first available Ethernet port of the Management Server to a Gigabit Ethernet port on the LAN.
- Then connect the first Ethernet port of each *ESXi Host Server* to a Gigabit Ethernet port on the campus LAN.

| vCenter Outside IP Address | |
|---|---|
| ESXi Management Server Outside IP Address | |
| ESXi Host Server 1 Outside IP Address | |
| ESXi Host Server 2 …6 Outside IP Address | |
| Subnet Mask | |
| Default Gateway | |
| Primary DNS Server | |
| Secondary DNS Server | |

### 1.5.2 Dual-Homed Networking

A Dual-Homed network model is used when you are hosting both virtual machines and real lab equipment for students to use. This model uses VLANS on NETLAB+ control switches which serve as an "inside" network for virtual machine traffic between each ESXi Host Server. All traffic flows across the campus LAN and all virtual machine traffic flows through the "inside" network.

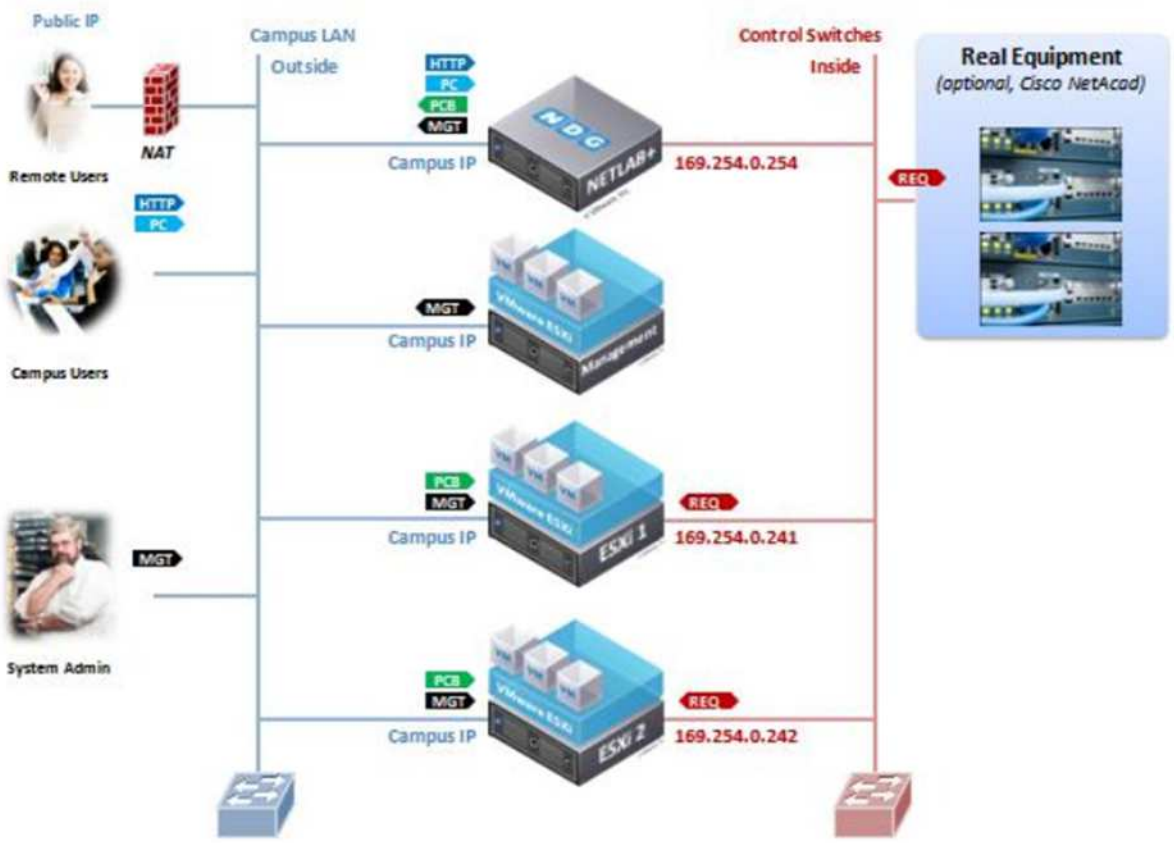



Diagram from Remote PC Guide Series – Volume 1 NetDevGroup.com

When allocating space for your Single-Homed network model, the following tasks need to be revised:

- First, obtain an IP address, subnet mask, and default gateway for each outside server interface connected to the campus LAN.
- Connect the first available Ethernet port of the Management Server to a Gigabit Ethernet port on the LAN.
- Then connect the first Ethernet port of each *ESXi Host Server* to a Gigabit Ethernet port on the campus LAN.

- Connect the second available Ethernet port of each *ESXi Host Server* to an available reserved port on a control switch.

Then you will need to console into the control switch and configure each "inside" *ESXi Host Server* switchport as a trunk.

```
Interface FastEthernet0/N
        description inside connection to ESXi Host Server #
        switchport mode trunk
        switchport mode nonnegotiate
```

| vCenter Outside IP Address | |
|---|---|
| ESXi Management Server Outside IP Address | |
| ESXi Host Server 1 Outside IP Address | |
| ESXi Host Server 1 Inside IP Address | |
| ESXi Host Server 2 ---6 Outside IP Address | |
| ESXi Host Server 2 ---6 Inside IP Address | |
| Outside Subnet Mask | |
| Inside Subnet Mask | |
| Outside Default Gateway | |
| Inside Default Gateway | |
| Primary DNS Server | |
| Secondary DNS Server | |

## 1.6 Connectivity

The placement of the NETLAB+ system needs to be either located on a public network or Demilitarized Zone (DMZ ). Now since NETLAB+ will most likely be installed behind a firewall, additional steps will need to be taken to open up some TCP/IP ports for functionality.

### 1.6.1 Internet Connection

NETLAB+ will need access to an internet connection. The minimum connection speed should be 500 kilobits per second in both directions following NDG's requirements. They encourage a T1 connection (1.5 Mbps) or higher following the deployment of remote PCs or virtual machines. Also, it is important to note that DHCP cannot be used. Instead, a static IP address will need to be assigned.

### 1.6.2 Network Address Translation (NAT)

NETLAB+ will work with Static Network Address Translation (NAT). This allows the use of matching a private IP address to a public IP address. However, Port Address Translation (PAT) and Dynamic NAT are not supported.

### 1.6.3 Outside to Inside Firewall Requirements

Remote users connect to the NETLAB+ server through the outside interface. NETLAB+ listens for connections on three TCP ports. If a firewall is placed in front of the NETLAB+ system, the following ports should be open.

| Ports | Usage |
|---|---|
| **TCP 80** | Access to the web-based user interface. |
| **TCP 2201**<br><br>(default) | Gives access for lab equipment and remote PC's. |
| **TCP 22**<br><br>(recommended) | Gives SSH access for NDG's technical support. |

### 1.6.4 Inside to Outside Firewall Requirements

The NETLAB+ server makes occasional outbound connections using the following ports.

| Ports | Usage |
|---|---|
| **TCP 25**<br><br>(optional) | Allows the NETLAB+ server to send email to users. |
| **TCP 80** | Allows the NETLAB+ server to connect to the NDG *Central Support System (CSS)*. This server is important as it provides software updates. |
| **UDP 53** | This port is used for when the NETLAB+ server makes DNS queries to resolve the address of the support server. |

More information regarding to connectivity requirements and firewall considerations can be found here: http://goo.gl/fjsBCK

# 2 Installing the NETLAB+ Server Appliance

## 2.1 Background

This section of the guide will help guide you through the process of installing a NETLAB+ server for the first time. When continuing on through the next sections, it is expected that the NETLAB+ server is already rack mounted.

## 2.2 Connect NETLAB+ to Outside Network

The NETLAB+ outside interface needs to be connected to your network. Make sure this cable is connected to Ethernet 0. The port should connect to a functional 10/100 port on your LAN.

## 2.3 How to Access the NETLAB+ Console

When choosing a console access method to perform basic IP configurations, you will need to connect to the NETLAB+ console interface. This can be done in two ways:

- Connect a VGA monitor and keyboard to the designated ports on your system. This method will allow you to easily observe what happens during the boot process.
- Establish a serial connection from another PC, laptop, or terminal using the server's built-in serial port and communications software (Putty, Hyper Terminal).

## 2.4 Connect to a Power Source

NETLAB+ needs to be connected to an un-switched, surge-protected outlet. Please be sure to not connect NETLAB+ to a switched outlet such as an APC device.

## 2.5 Accessing the Console

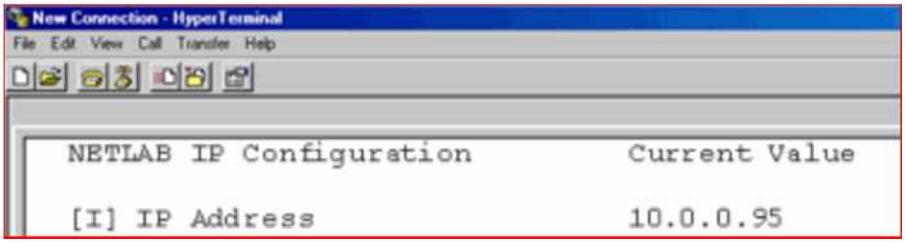
In this section, you will connect to the server console. Once connected, press the **Enter** key. When asked if you want to log in, respond **Yes**. Then a password prompt will be displayed for the administrator account. The default administrator password is **netlab**.

## 2.6 NETLAB+ IP Configuration

NETLAB+ will require a static IP address. If you are using Network Address Translation (NAT), a unique external IP address will need to be allocated to NETLAB+ along with opening a static mapping between the external and internal NETLAB+ IP addresses.

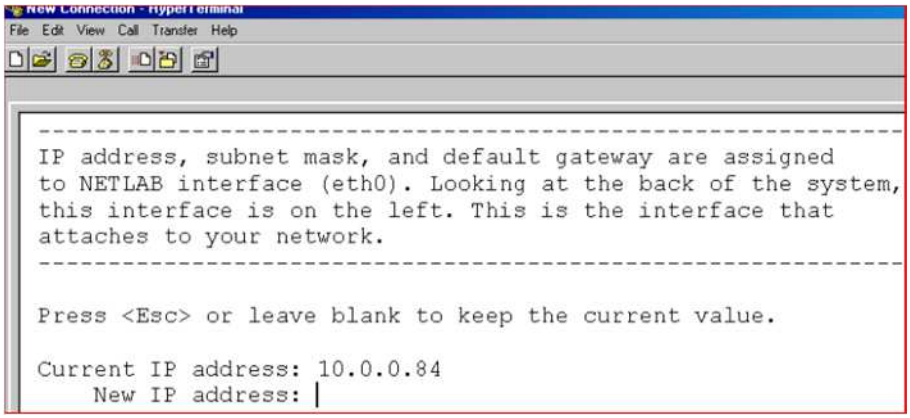
The following steps will help guide the process of configuring an IP address:

1. Make sure you have consoled into the NETLAB+ server appliance and logged in as administrator using the password **netlab**.
2. When viewing the main menu screen, enter "**I**" to access the *NETLAB+ IP Configuration* menu.



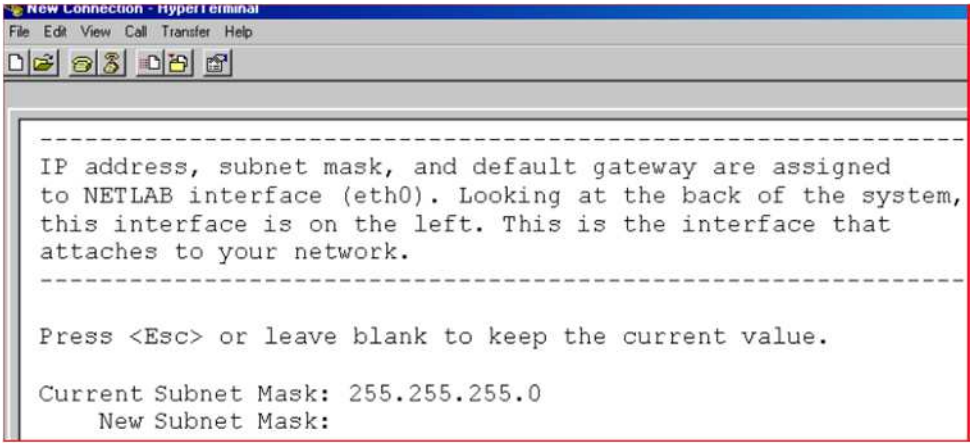

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

3. When prompted, enter your unique IP address in dotted decimal format.


File Edit View Call Transfer Help
IP address, subnet mask, and default gateway are assigned
to NETLAB interface (eth0). Looking at the back of the system,
this interface is on the left. This is the interface that
attaches to your network.
Press <Esc> or leave blank to keep the current value.
Current IP address: 10.0.0.84
New IP address:

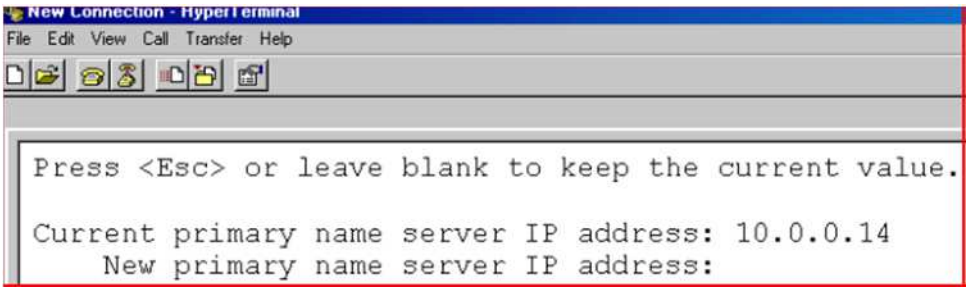
Referenced from NETLAB+ Installation Guide - NetDevGroup.com

4. Next, enter the values for the subnet mask and default gateway. Important note: The default gateway address must be on the same network as the IP address and subnet mask you assign.


New Connection - HyperTerminal
File Edit View Call Transfer Help
IP address, subnet mask, and default gateway are assigned
to NETLAB interface (eth0). Looking at the back of the system,
this interface is on the left. This is the interface that
attaches to your network.
Press <Esc> or leave blank to keep the current value.
Current Subnet Mask: 255.255.255.0
New Subnet Mask:

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

5. When asked to enter a primary name server, enter the IP address of the primary and then the backup DNS servers.


New Connection - HyperTerminal
File Edit View Call Transfer Help
Press <Esc> or leave blank to keep the current value.
Current primary name server IP address: 10.0.0.14
New primary name server IP address:

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

6. In the next section, you may define the remote access ports to use in place of the default remote access port selection, port 2201. You may leave this as default.

> *It is critical that the ports that are specified for remote access are opened on the network firewall. Failure to do so will result in port test failures during user login and delays. Remember that ports 22, 80, and 443 are reserved for other functions and cannot be used as remote access ports.*

7. Once the configurations are made, you must select the "**X**" option to exit and save the changes.

8. Once the values have been saved, a Network Test (option "**T**") should be initiated to test the connectivity.

> *For best practice, always perform a graceful shutdown from the system console or administrator web interface before powering down the NETLAB+ server.*

## 2.7 Outbound Firewall Test

In order to function properly, NETLAB+ must be able to send certain traffic through the network. The outbound traffic includes DNS lookups, outbound mail, and HTTP to the *NDG Central Support System (CSS)*.

A NETLAB+ Outbound Network and Firewall Test should be initiated to determine if the interface, gateway, and DNS are reachable. If any errors are displayed during the test, they need to be evaluated and corrected. Usually, most of the errors are caused by firewall configuration issues.

A successful test will indicate **OK** for all test types.

```
NETLAB Outbound Network and Firewall Test…

Test    Protocol/Port      Destination           Status
----    -------------      ----------------      ---------------
ping    icmp (echo)        primary interface     RUNNING - OK (5/5)
ping    icmp (echo)        default gateway       RUNNING - OK (5/5)
ping    icmp (echo)        primary DNS           RUNNING - OK (5/5)
find    dns (53 udp)       nss.intranet          RUNNING - OK (10.0.0.82)
ping    icmp (echo)        nss.intranet          RUNNING - OK (5/5)
get     http (80 tcp)      nss.intranet          RUNNING - OK
mail    smtp (25 tcp)      mail.netdevgroup.com RUNNING - OK

Tracing the route from this server to CSS.
This may fail if ICMP echo packets are blocked.
traceroute to nss.intranet (10.0.0.82), 30 hops max, 38 byte packets
 1 nss.intranet (10.0.0.82) 0.345 ms 0.311 ms 0.307 ms

Press any key to continue…
```

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

## 2.8 Connecting to the NETLAB+ Web-Based Interface

Once the IP configuration is completed, you will be able to access the web-based interface. This is where you will perform the reminder of your configuration tasks.

Using a PC connected to the same LAN as the NETLAB+ appliance, open a web browser and type the IP address you assigned to the NETLAB+ appliance.

## 2.9 Logging into NETLAB+ as an Administrator

The web browser should display a NETLAB+ login page. You may login with the administrator credentials. When prompted for the username and password, login as **administrator** using the default password **netlab**.

You will be required to change the password. Create a secured password using the minimum requirements:

- Not found in the dictionary and not too simple
- Between 7 and 16 characters
- Contain both numbers and letters

## 2.10 Remote Access Test

A remote access test is performed each time a user logs on. This is a preliminary step to make sure that your PC will be able to make a connection to NETLAB+ for remote device access and remote PC access.

This is a crucial step to be able to access NETLAB+ correctly. If an issue rises, it needs to be corrected. Things to look for may include:

- **Personal firewall settings on your computer**: The host firewall may be blocking a connection to the port 2201 (default) or whichever remote access port was assigned for NETLAB+ depending on your configuration.
- **Security policy at your current location**: It can be possible that the network firewall does not allow outbound access using the port(s) chosen by the NETLAB+ administrator.
- **Port may not have been opened in the site firewall**: Verify that the network administrator has opened the required ports for outbound client connections.

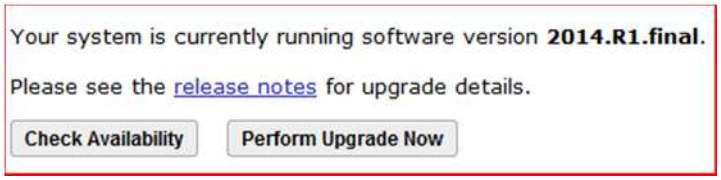
## 2.11 Check for Software Updates

It is recommended to check for software updates at this time. The NETLAB+ appliance was shipped with the latest software version but it may be possible that a new software update may have become available while the server was on route to your site.

The following steps will help guide the process of updating software on a NETLAB+ appliance:

1. Login into the administrative page of your NETLAB+ system.
2. Select the **Software Updates** icon.

3. Click on **Check Availability**.
4. The NETLAB+ appliance will now query to the *Central Support System (CSS)* to see if an updated version exists. If an updated version is available, select **Perform Upgrade Now**.

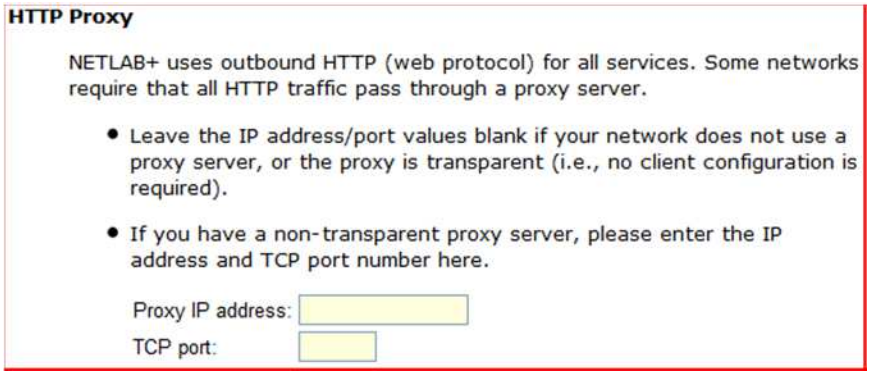

Your system is currently running software version 2014.R1.final.
Please see the release notes for upgrade details.
Check Availability
Perform Upgrade Now

## 2.12 Configure NETLAB+ Services

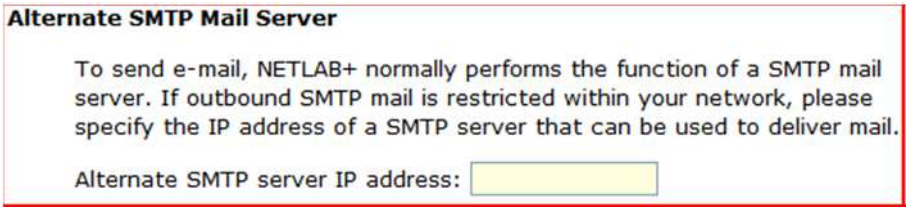
NETLAB+ offers a few different services such as *Backup Service*, *Software Update Service*, and *Time Service*. These can be accessed via the administrative page by clicking the **Configure Services** icon.

These services are enabled by default per NDG recommendations, but can be disabled if necessary.

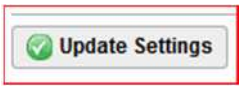
If your network has a non-transparent proxy server, you must enter the IP address and TCP port number in the indicated fields. These are only required for proxy servers that are non-transparent. If changes are made, be sure to select **Update Settings** when finished.


HTTP Proxy
NETLAB+ uses outbound HTTP (web protocol) for all services. Some networks require that all HTTP traffic pass through a proxy server.
Leave the IP address/port values blank if your network does not use a proxy server, or the proxy is transparent (i.e., no client configuration is required).
If you have a non-transparent proxy server, please enter the IP address and TCP port number here.
Proxy IP address:
TCP port:

NETLAB+ offers SMTP services to deliver email to administrators and instructors. If email delivery is restricted within your network to a specific SMTP server, you can configure NETLAB+ to use the SMTP servers at your site to deliver email.


Alternate SMTP Mail Server
To send e-mail, NETLAB+ normally performs the function of a SMTP mail server. If outbound SMTP mail is restricted within your network, please specify the IP address of a SMTP server that can be used to deliver mail.
Alternate SMTP server IP address:

If any changes are made, be sure to click the Update Settings button to save the settings.




## 2.13 NETLAB+ Maintenance Reminder

Every NETLAB+ system displays the status of your system maintenance agreement. The maintenance fee covers the cost of technical support and software updates. The last day of your current maintenance agreement is displayed in the upper right-hand corner when on the main administrator page.

More information about the maintenance agreement can be found here:
http://goo.gl/v2tgdC

# 3 Configuring BIOS and RAID Configuration

## 3.1 Background

This section of the guide helps configure the VMware hosts servers. For reference, this step-by-step walkthrough has been tailored for the Dell R720. Please consult the user manual provided by the manufacturer of your server for proper configuration.

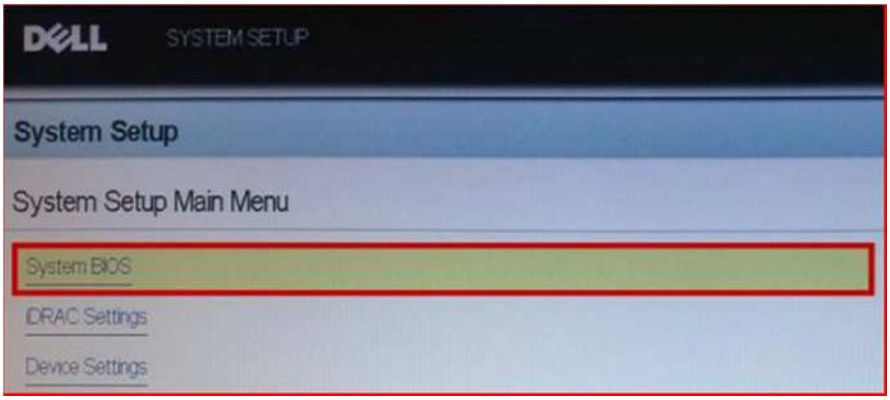
## 3.2 BIOS Changes

Follow the instructions to prep your server for virtualization.

1. Turn on or restart the system.
2. Press **F2** to enter the *System Startup* at the BIOS startup screen.

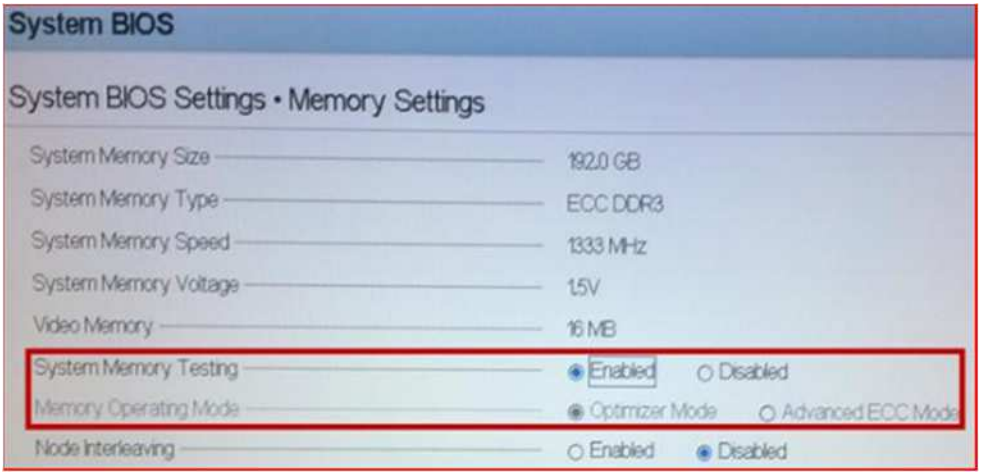
Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

3. Select **System BIOS** from the *System Startup Main Menu*.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

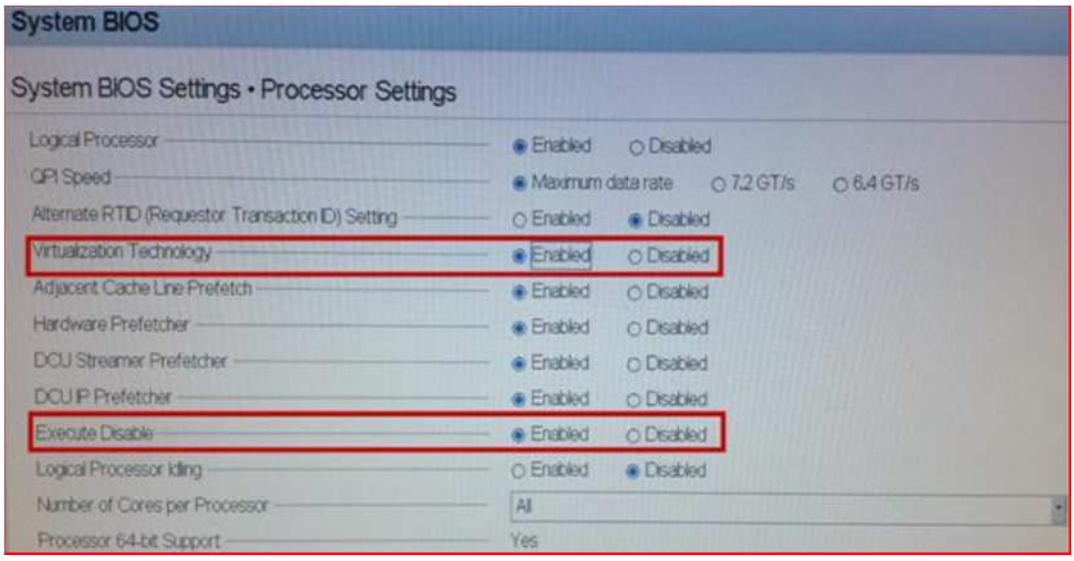
4. Using the arrow keys, select **Memory Settings** and make sure *System Memory Testing* is **Enabled** and *Memory Operating Mode* is set to **Optimizer Mode**.


System BIOS
System BIOS Settings • Memory Settings
System Memory Size 192.0 GB
System Memory Type ECC DDR3
System Memory Speed 1333 MHz
System Memory Voltage 1.5V
Video Memory 16 MB
System Memory Testing Enabled Disabled
Memory Operating Mode Optimizer Mode Advanced ECC Mode
Node Interleaving Enabled Disabled

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

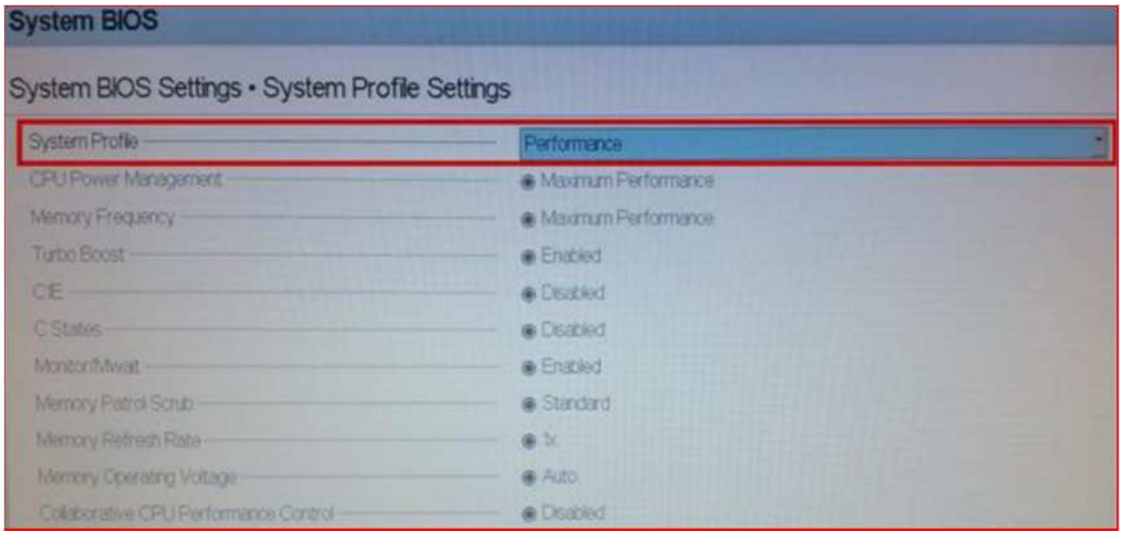
5. Press **Esc** to return to the main menu.

6. Using the arrow keys, select **Processor Settings** and make sure *Virtualization Technology* is set to **Enabled** and *Execute Disable* is set to **Enabled**.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

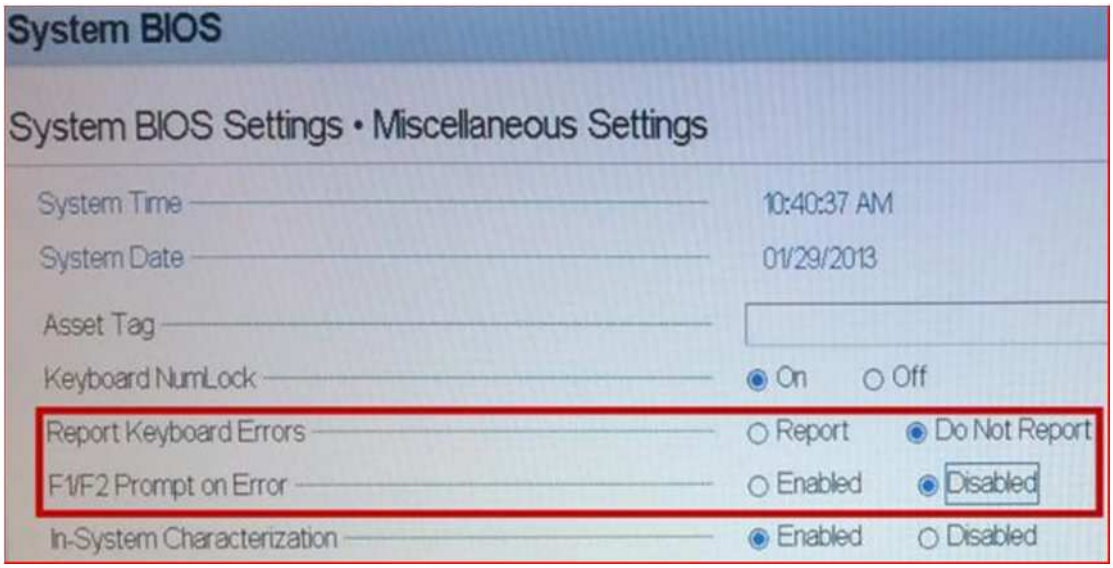
7. Press **Esc** to return to the main menu.
8. Using the arrows keys, select **System Profile Settings** and make sure *System Profile* is set to **Performance**.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

9. Press **Esc** to return to the main menu.

10. Using the arrow keys, select **Miscellaneous Settings** and make sure *Keyboard Errors* is set to **Do Not Report** and *F1/F2 Prompt on Error* is set to **Disabled**.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

11. Press **Esc** to return to the main menu.
12. Make sure to save settings and exit.

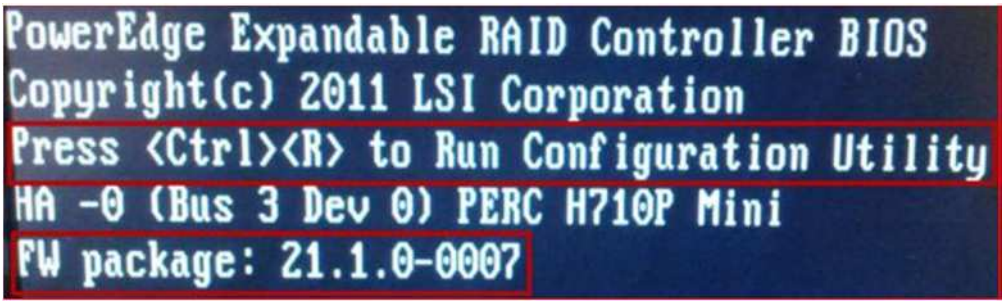
## 3.3 RAID Configuration

NDG has tested and recommends the configuration for an eight drive setup to be used with RAID 5. This configuration helps maximize write speeds and pod count per host. This will help support courses that require high Input/Output Operations per Second (IOPS). The quality of the RAID controller is important and so NDG has recommended the H710P RAID controller with 1GB cache.

A brief overview of RAID 5 is that its process is known as striping with parity. It is important to remember that RAID 5 requires a minimum of 3 drives. RAID 5 can only tolerate one disk failure; a two disk failure will cause the array to fail.

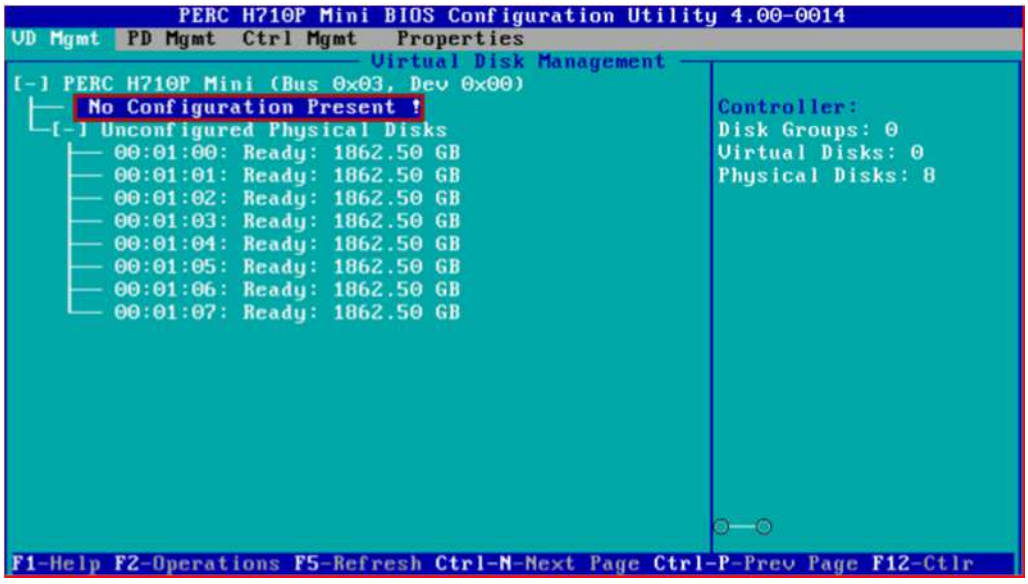
### 3.3.1 RAID Configuration Utility - 8x2TB HDD using RAID 5

1. Turn on or restart the system.
2. During the boot process, a short dialogue will appear *Press <Ctrl><R> to Run Configuration Utility*. Once this message displays, press **Ctrl+R**.


PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2011 LSI Corporation
Press <Ctrl><R> to Run Configuration Utility
HA -0 (Bus 3 Dev 0) PERC H710P Mini
FW package: 21.1.0-0007

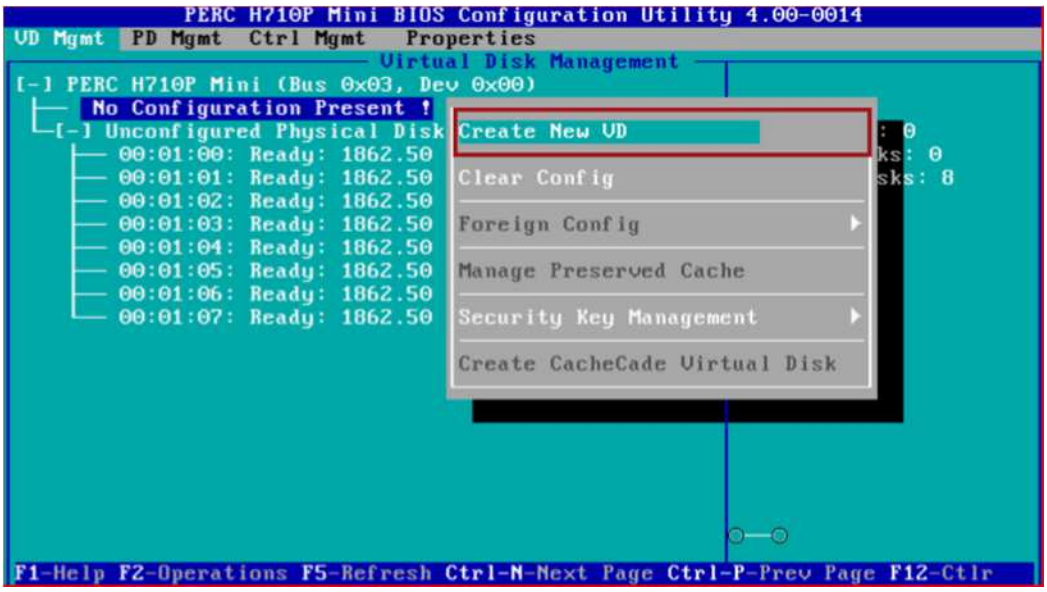
Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

3. Clear any existing configurations.
4. Once you start with a clean configuration, go ahead and select **No Configuration Present**. Then press **F2**.


PERC H710P Mini BIOS Configuration Utility 4.00-0014
VD Mgmt PD Mgmt Ctrl Mgmt Properties
Virtual Disk Management
[-] PERC H710P Mini (Bus 0x03, Dev 0x00)
No Configuration Present !
[-] Unconfigured Physical Disks
00:01:00: Ready: 1862.50 GB
00:01:01: Ready: 1862.50 GB
00:01:02: Ready: 1862.50 GB
00:01:03: Ready: 1862.50 GB
00:01:04: Ready: 1862.50 GB
00:01:05: Ready: 1862.50 GB
00:01:06: Ready: 1862.50 GB
00:01:07: Ready: 1862.50 GB
Controller:
Disk Groups: 0
Virtual Disks: 0
Physical Disks: 8
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr

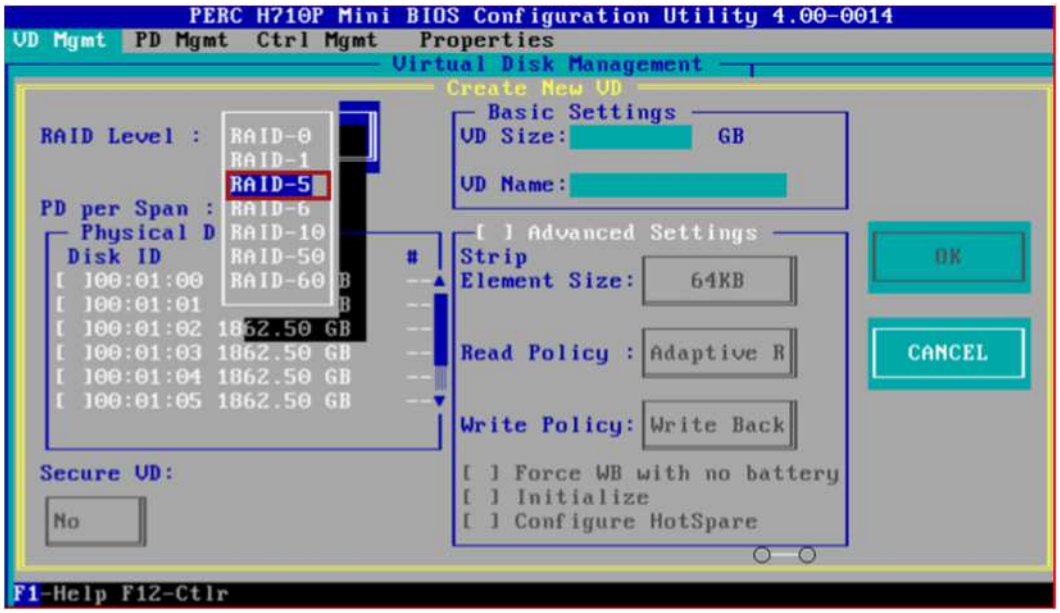
Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

5. Select **Create New VD** and press **Enter**.



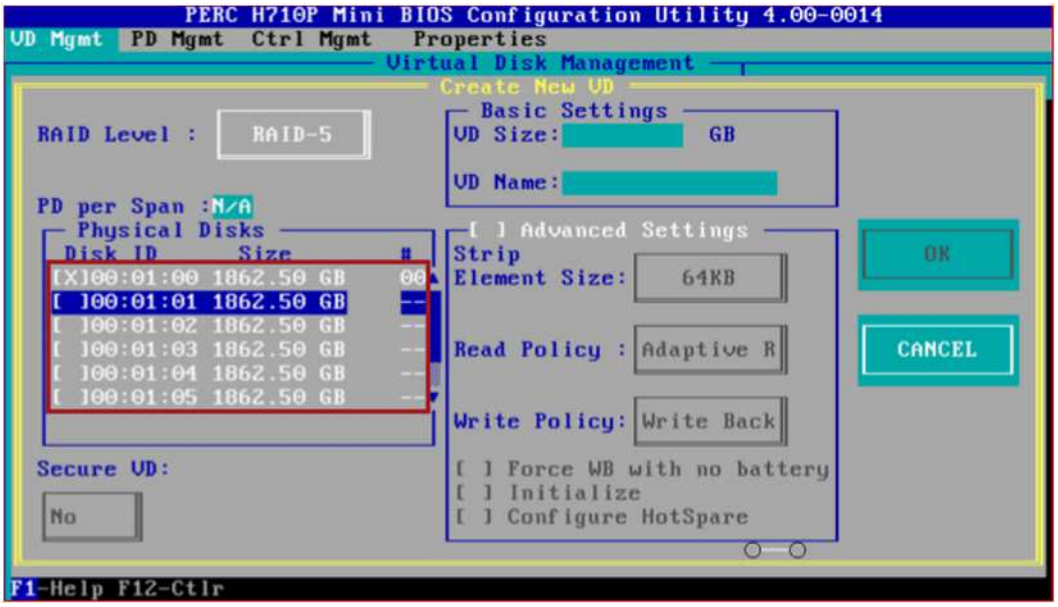

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

6. Use your **Tab** key to reach *RAID Level* and select **RAID-5.**



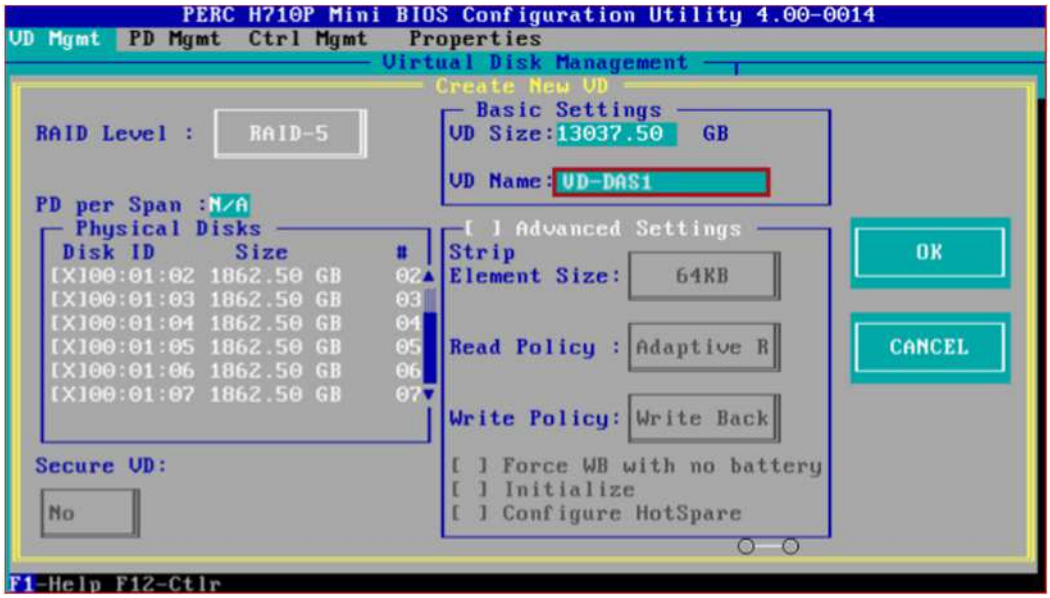

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

7. Use the **Tab** key again to reach *Physical Disks* this time and select all available disks by pressing the **space bar** to put a checkmark next to the available disks.



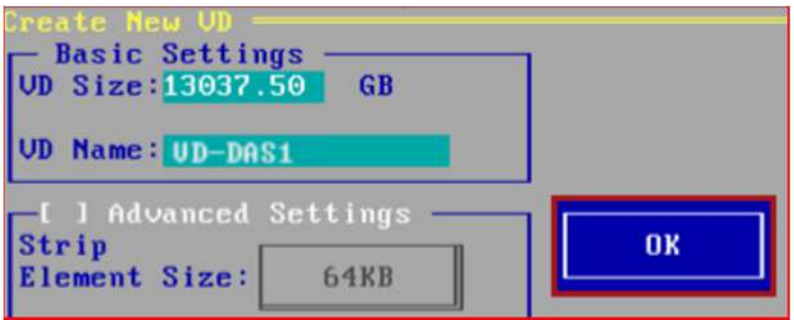

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

8. Use the **Tab** key again to reach the *VD Name* field and type the name of your volume. This can be anything as it reflects to your naming convention.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

9. Select **OK** on the right once you are ready to proceed.



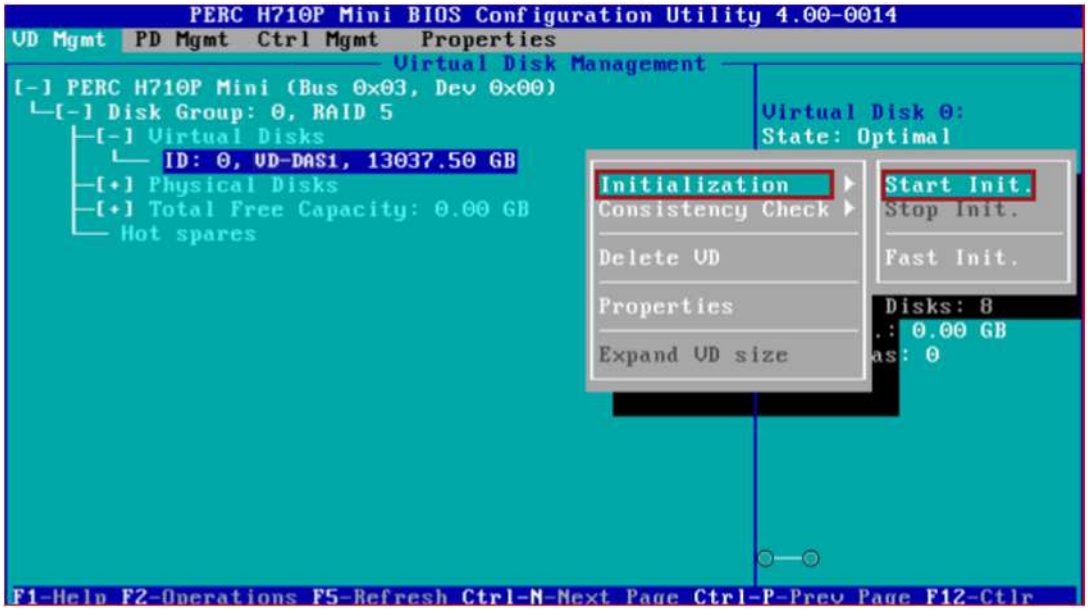

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

10. A popup message will appear stating that we need to initialize the virtual disk after it has been configured. Select **OK**.

It is recommended that all newly created logical drives be initialized unless you are attempting to recreate a previous configuration and recover data as initialization is a destructive process.
OK

Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

11. Using the arrow keys, highlight the newly created Virtual Disk (this will vary depending on the name that you have used in the previous step.). Press **F2** and select **Initialization** > **Start Init**. Then select **Yes** to confirm the initialization of the disks. This process may take several hours depending on your disk setup.




Referenced from NETLAB+ Remote PC Guide Series – Volume 2b NetDevGroup.com

12. If you are prompted to continue, select **Yes** followed by pressing the **Enter** key.
13. You may press the **Enter** key on the *Virtual Disk* to see the estimated time remaining until the process finishes.
14. Once initialization is complete, select **OK** to confirm.
15. Press **Esc** to close out of the *RAID Configuration Utility*. When exiting, select **OK** to confirm.
16. You will then be prompted to reboot your system.

# 4 VMware ESXi Server Setup

## 4.1 Background

This section of the guide will help guide you in the process of installing ESXi software on the host servers. There should be a recommended number of two ESXi host servers. One will be used for management, referred to as the Management Server and the other will be the *ESXi Host Server* which will inventory the virtual machines for the pods. You may have more ESXI host servers if you plan on teaching a larger number of classes that would require more virtual machines to be hosted.

## 4.2 Preparing the ESXi Server

It is important to note that Section 2: Configuring BIOS and RAID Configuration needs to be completed before moving on.

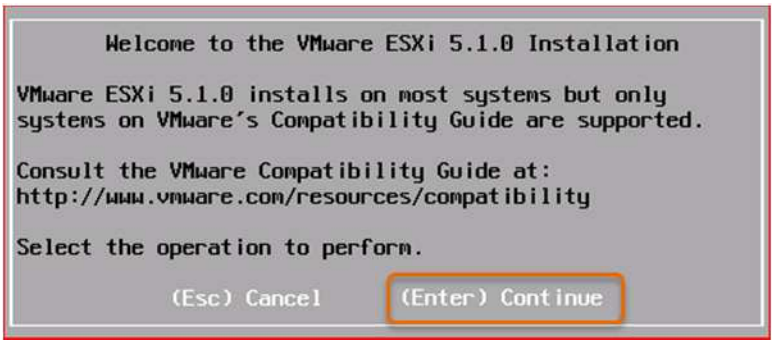
## 4.3 Installing the ESXi Server

This section will walk you through the installation of VMware ESXi to your Management Server(s) and to each ESXi Host Server(s).

> *Before proceeding, please make sure to have a burned copy of the ESXi 5.1 Installable ISO if you have not done so already.*

Follow the instructions to install ESXi:

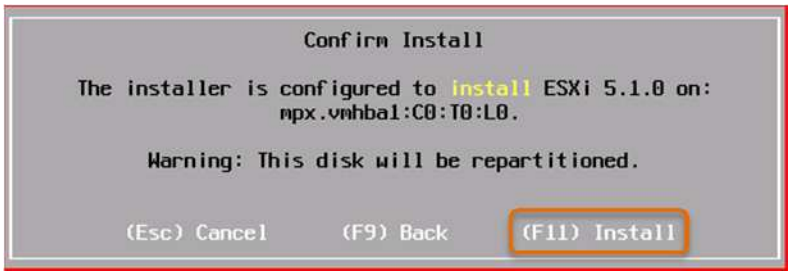
1. Turn on the system.
2. Insert the ESXi 5.1 media (CD).
3. When represented with the welcome screen, press **Enter** to continue.


Welcome to the VMware ESXi 5.1.0 Installation
VMware ESXi 5.1.0 installs on most systems but only
systems on VMware's Compatibility Guide are supported.
Consult the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility
Select the operation to perform.
(Esc) Cancel
(Enter) Continue

4. An *End User License Agreement (EULA)* screen is displayed. Press **F11** to accept and continue.

5. On the *Select a Disk* screen, choose the available Dell PERC drive. The capacity will vary depending on the configuration setup you chose to implement. Once the drive is highlighted, press **Enter** to continue.
6. Make sure **US Default** is selected for the keyboard layout and press **Enter** to continue.

7. The next screen will prompt you to set a root password. Enter a password you wish to use. Press **Enter** once the fields are populated.
8. Press **F11** to begin the installation.




9. When the *Installation Complete* window appears, press **Enter** to reboot the machine.

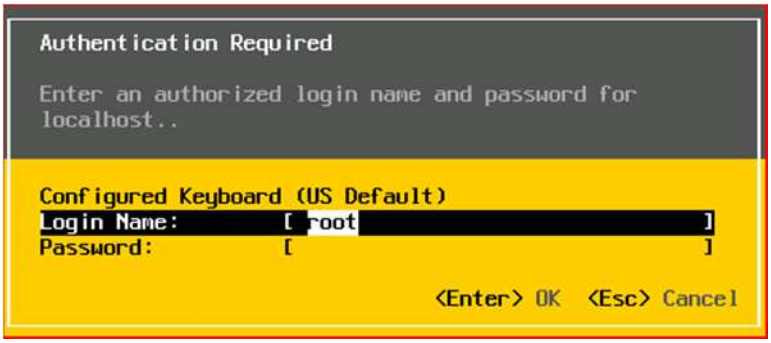
Installation Complete
ESXi 5.1.0 has been successfully installed.
ESXi 5.1.0 will operate in evaluation mode for 60 days. To use ESXi 5.1.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.
Remove the installation disc before rebooting.
Reboot the server to start using ESXi 5.1.0.
(Enter) Reboot

10. You have just successfully installed ESXi on your server, please make sure to repeat the steps for all of your management servers and host servers.

## 4.4 Basic Network Configuration

This section will help guide you in setting up basic network configurations for both management servers and host servers.

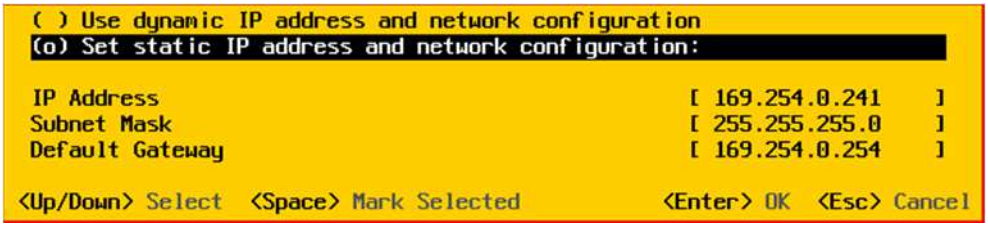
1. Once the ESXi is booted, you are prompted with a yellow and grey console screen. Press **F2** to begin setting up the server.
2. When prompted with a login screen, make sure the username is **root** with the password you have chosen in Section 3.3.


Authentication Required
Enter an authorized login name and password for localhost..
Configured Keyboard (US Default)
Login Name: [ root ]
Password: [ ]
<Enter> OK <Esc> Cancel

3. When viewing the *System Customization* menu, select **Configure Management Network** and press **Enter**.

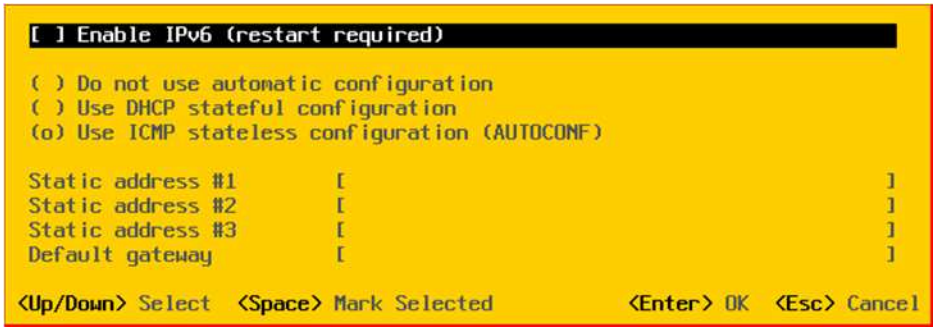
4. Select **IP Configuration** followed by pressing **Enter**.

5. Select **Set Static IP address and network configuration** and set the **IP Address**, **Subnet Mask**, and **Default Gateway** to an inside or outside IP configuration to fit your network configuration and model. You should have a table already listed with an IP addressing scheme in place. Press **Enter** to save settings.


( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:
IP Address [ 169.254.0.241 ]
Subnet Mask [ 255.255.255.0 ]
Default Gateway [ 169.254.0.254 ]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

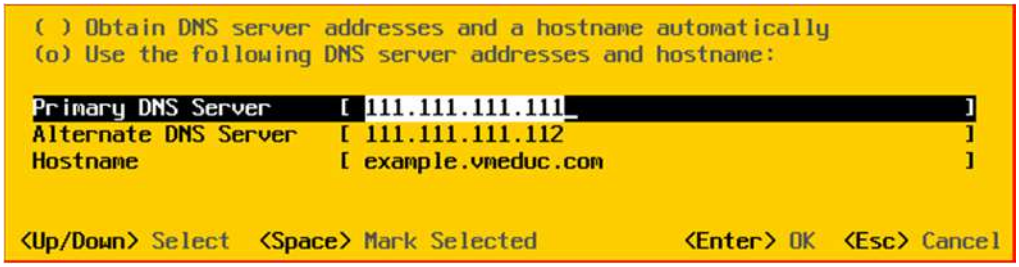
6. It is strongly suggested to disable IPv6 if not in use. Select **IPv6 Configuration** from the *Configure Management Network* menu.

7. Make sure **Enable IPv6** is highlighted and press the **spacebar** to remove the **X** from the checkbox. Press **Enter** to save settings (restart may be required).


[ ] Enable IPv6 (restart required)
( ) Do not use automatic configuration
( ) Use DHCP stateful configuration
(o) Use ICMP stateless configuration (AUTOCONF)
Static address #1 [ ]
Static address #2 [ ]
Static address #3 [ ]
Default gateway [ ]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

8. Next, you will want to set the DNS by selecting **DNS Configuration** from the *Configuration Management Network* menu.

9. Fill in the fields next to **Primary DNS** and **Secondary DNS**. For the **Hostname** you will want to name the server based on your naming conventions. Press **Enter** to save settings.


( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:
Primary DNS Server [ 111.111.111.111 ]
Alternate DNS Server [ 111.111.111.112 ]
Hostname [ example.vmeduc.com ]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

10. Press **Enter** again to confirm changes and return to the *Configure Management Network* menu.

11. Press **Esc** to exit. When prompted to *Apply changes and restart management network*, press **Y** to continue.

## 4.5 Request for NDG Optimized vCenter Server Appliance

In the following sections of the guide, you will be introduced to deploying and configuring the *NDG Optimized vCenter Server Appliance*. This appliance is recommended by NDG to be used with any NETLAB+ environment. You may request the appliance by filling out the following form: http://goo.gl/CQ2KyX

## 4.6 Installing the vSphere Client

*vSphere Client* needs to be installed on a Windows PC which will be used to manage the *vSphere* infrastructure.

The following steps will help guide you in installing the vSphere Client.

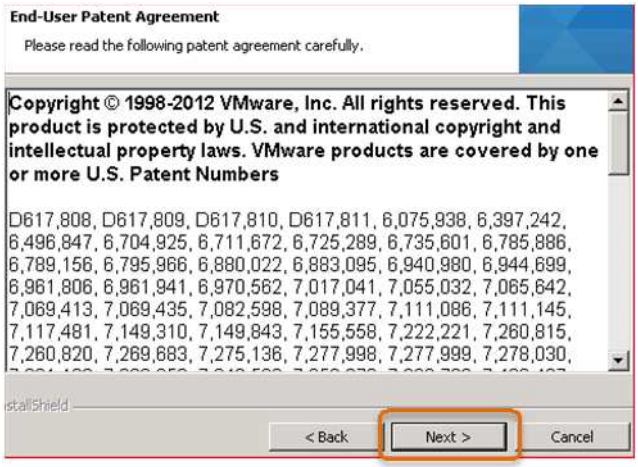
1. Open a web browser and go to http://*your-esxi-management-server-ip-address*.
2. Depending on your browser, you might be presented with a security certificate issue. Click on the option to ignore, understand the risk, add exception, proceed anyway, or otherwise agree to the non-trusted security certificate.
3. You will then be presented with a *VMware ESXi 5.1* screen. Click on the **Download vSphere Client** hyperlink.

VMware ESXi 5.1
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client

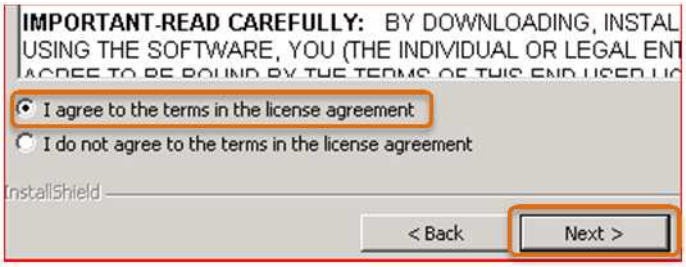
4. Save the installer to your desktop. Double-click the installer to start the installation.
5. If a security warning message appears, click on **Run**.
6. Extraction of files will initiate. Once that finishes, make sure **English** is selected and click **OK** to proceed.

VMware vSphere Client 5.1 - InstallShield Wizard
Select the language for the installation from the choices below.
English (United States)
OK
Cancel

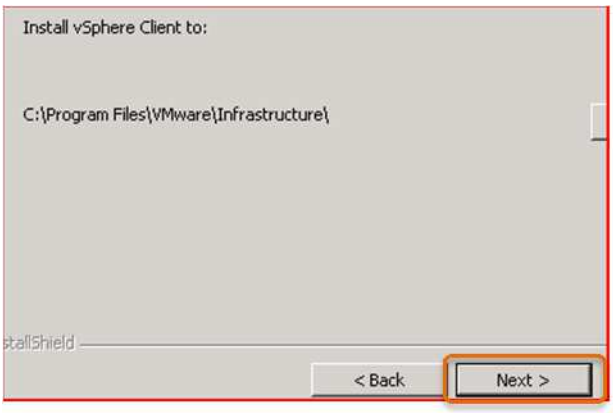
7. Click **Next** to continue.
8. Click **Next** to accept the *End-User Patent Agreement*.




9. Click **I agree to the terms in the license agreement** and click **Next** to continue.


IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTAL
USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENT
I agree to the terms in the license agreement
I do not agree to the terms in the license agreement
InstallShield
< Back
Next >

10. Accept the default destination folder by clicking **Next**.




11. Click **Install** to continue.
12. Click **Finish** to finish the installation.

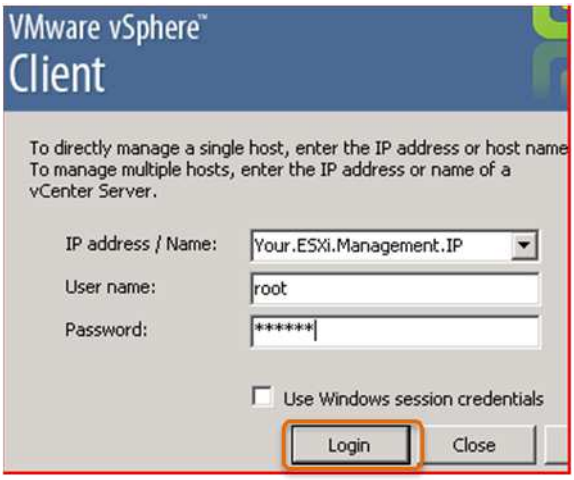
## 4.7 Deploying vCenter Server Appliance

In this section, you will be deploying the *NDG Optimized vCenter Server Appliance* on the *ESXi Management Server*. Make sure you have downloaded the optimized appliance, if you haven't done so, please refer to Section 4.5

The following steps will help guide you in deploying the *vCenter Server Appliance*:

1. Double-click on the **VMware vSphere Client** shortcut located on the desktop.

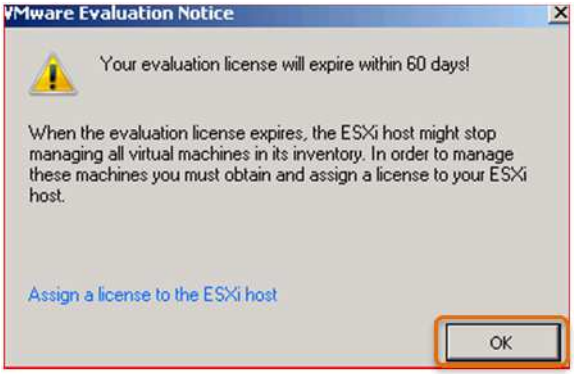
2. In the new window, enter the IP address of your ESXi Management Server (reference to your IP addressing table used in Section 1.5), with the username as **root** and the password that you have chosen in Section 3.3).




3. If a security warning is displayed, place a checkmark next to **Install this certificate and do not display any security warnings for "server_ip"** and click **Ignore**.

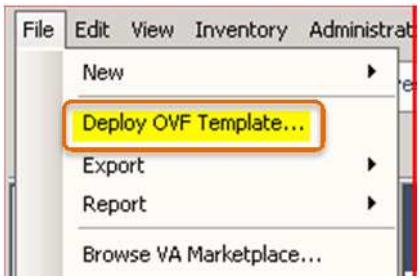
Certificate Warnings
An untrusted SSL certificate is installed on "172.16.1.51" and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern. You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.
The certificate received from "172.16.1.51" was issued for "localhost.localdomain". Secure communication with "172.16.1.51" cannot be guaranteed. Ensure that the fully-qualified domain name on the certificate matches the address of the server you are trying to connect to.
Click Ignore to continue using the current SSL certificate.
View Certificate
Ignore
Cancel
Install this certificate and do not display any security warnings for "172.16.1.51".

4. When prompted with the *VMware Evaluation Notice*, click **OK** to continue.


VMware Evaluation Notice
Your evaluation license will expire within 60 days!
When the evaluation license expires, the ESXi host might stop managing all virtual machines in its inventory. In order to manage these machines you must obtain and assign a license to your ESXi host.
Assign a license to the ESXi host
OK

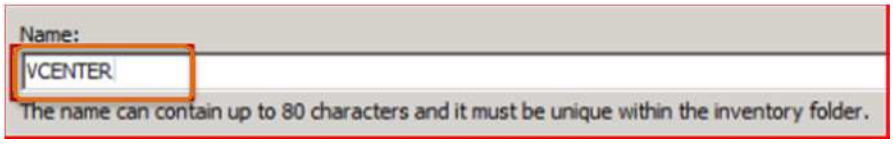
5. Once the *VMware Client* initiates, click the **Inventory** icon in the *main workspace* area.

6. Make sure to select the appropriate **ESXi host** on the left side of the tree view. Click **File** on the top menu bar and select **Deploy OVF Template…**

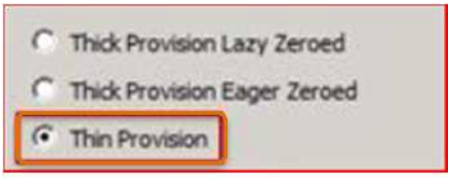



7. When the source window appears, click on **Browse…**

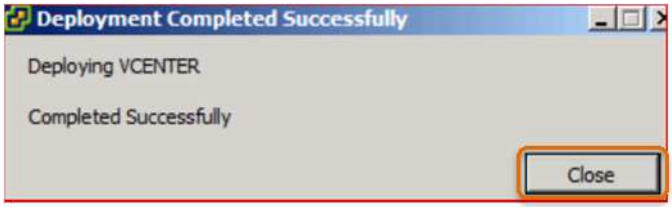
8. Another window will appear. Click **Desktop** in the left pane, and then click the **OVA** file you downloaded from *Section 4.5* (the file location is dependent on where you saved the downloaded file, "Downloads" may be another common option.). Click **Open**.
9. Click **Next** to continue.
10. On the *OVF Template Details* window, review that the information is correct and click **Next**.
11. On the *Name and Location* window, enter **VCENTER** in the *Name* field and click **Next**.



12. On the *Disk Format* window, select **Thin Provision** and click **Next**.




13. On the *Ready to Complete* windows, click **Finish** to deploy the *vCenter Server Appliance*.
14. Wait for the progress window to complete (this may take a few minutes). Click on **Close** when it has completed.

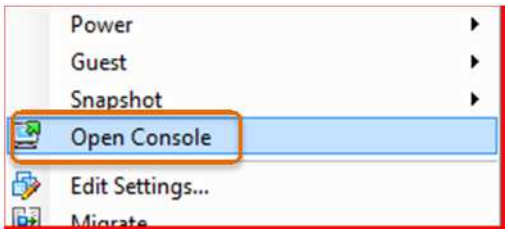



## 4.8 Configuring Network Settings

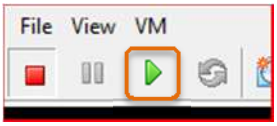
This section will help guide the IP configuration via the console on *VCENTER*. NDG strongly recommends you use a static IP address.

The following steps will help guide you in configuring the IP address:

1. Login to *vCenter* using the *vSphere Client*.
2. In the *vSphere Client*, expand the ESXi host on the left to display the *VCENTER* appliance.
3. Right-click on **VCENTER** and select **Open Console**.

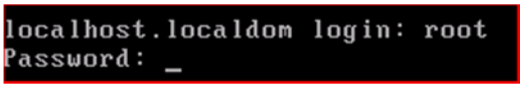


4. Click the **Power On** button in the toolbar to power on the VM.



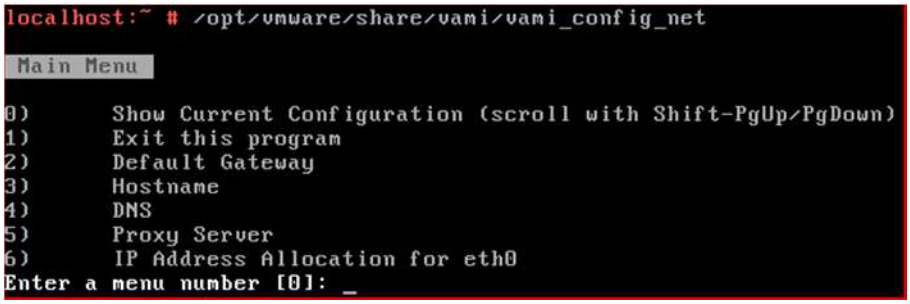

5. Once the appliance has finished booting up, you will configure the network settings manually. Make sure **Login** is selected towards the bottom and press **Enter**.

6. Enter **root** for the username and enter **vmware** for the password.




7. Enter the following command:

```
localhost:~# /opt/vmware/share/vami/vami_config_net
```




8. A numbered menu will appear. Type **6** and press **Enter** to set the *IP Address Allocation for eth0*.

9. When prompted to "*Configure an IPv6 address for eth0?*" press **Enter** to select the default.

```
Configure an IPv6 address for eth0? y/n [n]: _
```

10. When prompted to "Configure an IPv4 address for eth0?" type **y** and press **Enter**.

```
Configure an IPv4 address for eth0? y/n [n]: n
```

11. When prompted to "*Use a DHCPv4 Server instead of a static IPv4 address?*" type **n** and press **Enter**.

```
Use a DHCPv4 Server instead of a static IPv4 address? y/n [y]: n
```

12. Enter your IP address for the *IPv4 Address* and press **Enter**.

```
IPv4 Address []: your.vcenter.IP.address
```

13. Enter your subnet mask for the *Netmask* and press **Enter**.

```
Netmask []: 255.255.255.0
```

14. When asked "*Is this Correct?*" say yes by pressing **Enter**.

```
Is this correct? y/n [y]: _
```

15. To set the *Default Gateway*, type **2** and press **Enter**.

```
Enter a menu number [0]: 2_
```

16. When prompted to select the interface, press **Enter** to select the defaults.

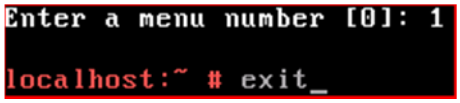
```
Warning: if any of the interfaces for this VM use DHCP,
the Hostname, DNS, and Gateway parameters will be
overwritten by information from the DHCP server.

Type Ctrl-C to go back to the Main Menu

0)      eth0
Choose the interface to associate with default gateway [0]: _
```

17. Enter the *IPv4 Default Gateway* and press **Enter**.

```
IPv4 Default Gateway []: your.default.gateway.IP_
```

18. Make sure to leave the *IPv6 Default Gateway* blank and press **Enter**.

19. Once the changes have been made, type **1** on the *Main Menu* and press **Enter** to exit.




## 4.9 Creating a NETLAB+ User on the vCenter Appliance

This section of the guide will show you how to create a NETLAB+ user account for NETLAB+ to access your *VCENTER*.

The following steps will help guide you in creating a user account for NETLAB+:

1. While still in the command prompt of the *vCenter Server Appliance*, enter the following command to add a NETLAB user account:

```
localhost:~#  useradd –m NETLAB
```

2. Enter the following command to change the password:

```
localhost:~#  passwd NETLAB
```

3. Enter a password of your choice and then retype the new password to confirm.
4. Enter the following command to edit the password policy:

```
localhost:~#  chage NETLAB
```

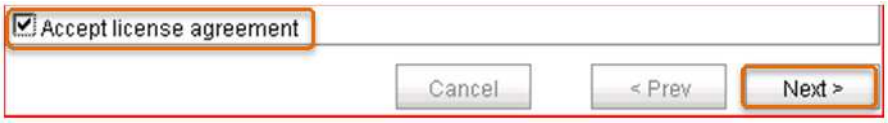
5. Set the following values for each option:
   a. Minimum Password Age: **0**
   b. Maximum Password Age: **99999**
   c. Password Expiration Warning: **7**
   d. Password Inactive: **-1**
   e. Account Expiration Date: **-1**
6. Type **exit** and press **Enter** to log out of the console.
7. Depress **CTRL+ALT** to release the mouse from the VM.
8. Click the File menu and select Exit to close the console.

## 4.10 vCenter Appliance Initial Configuration

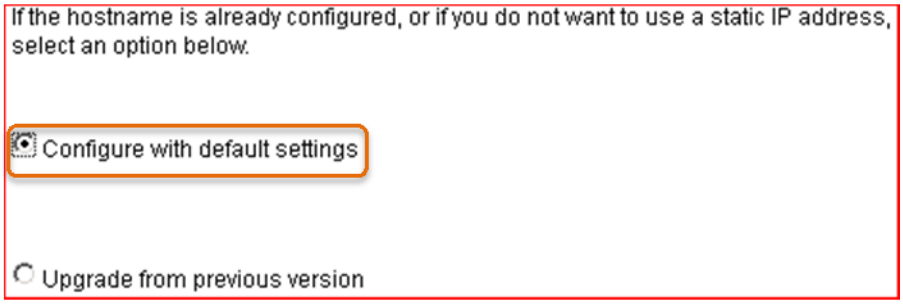
The following steps will help guide you in conducting initial configuration on the *vCenter Appliance*:

1. Open an internet browser.
2. In the *address bar*, enter **https://yourvcenteripaddress:5480**. Depending on your browser, you will be displayed with a security certificate issue. Click on the option to ignore, understand the risk, add exception, proceed anyway, or otherwise agree to the non-trusted security certificate.
3. When asked to enter login credentials, enter **root** as the username and **vmware** for the password. Click **Login**.

4. Select the **checkbox** next to *Accept license agreement*. Click **Next**.




5. Select **Configure with default settings** and click **Next**.


If the hostname is already configured, or if you do not want to use a static IP address, select an option below.
Configure with default settings
Upgrade from previous version

6. Review the information and click **Start** to configure the *vCenter* with default settings (this may take a few minutes).
7. You will now be presented with a *Summary* screen. Wait until everything has loaded to proceed onto the next section.

## 4.11 Setting Hostname and Changing the root Password

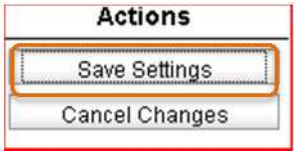
The following steps will help guide you in changing the hostname of the *vCenter Appliance*, enabling *Certificate Regeneration*, and changing the root password.

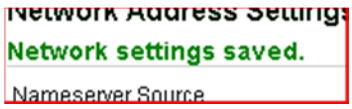
1. Make sure you are still logged into the VMware vCenter Server Appliance through your web browser. If not, repeat steps 1 through 3 from section 4.10.
2. Click on the **Network** tab at the top while logged into the *vCenter Appliance* through web browser.

3. Click the **Address** tab below.

4. In the *Hostname* field, enter **VCENTER**.

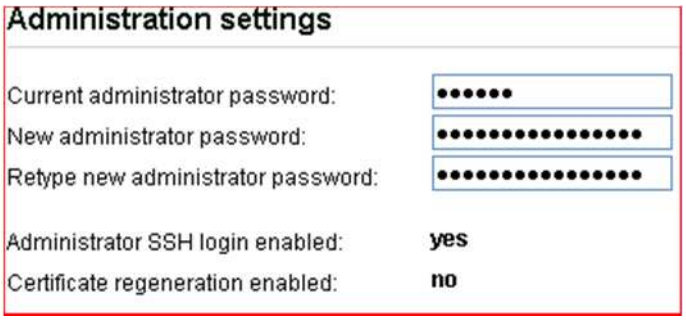
5. Click **Save Settings**, under *Actions* on the right-hand side. Wait for the notice in green that indicates that the network settings have been saved.



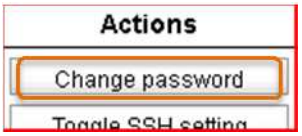




6. Click on the **Admin** tab at the top.

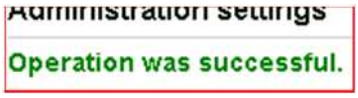
7. Change the administrator password:




   a. In the *Current administrator password* field, type **vmware**.
   b. In the *New administrator password* field, choose a new password for the *vCenter Appliance*.
   c. Type the same password in the *Retype new administrator password* field.
   d. Click on the **Change password** button to save.




8. Click on the **Toggle certificate setting** button to change the Certificate regeneration. You should notice the *Certification regeneration enabled* option changed to **yes** and a green notification "*Operation was successful*" will appear above the *Current administrator password* field.




9. Click **Logout** user root in the upper-right corner.

10. Close your browser and maximize the *vSphere Client* window.

11. Right-click on the **VCENTER** in the inventory list and select **Open Console**.

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

12. Click the **Restart Guest** button to restart the *VCENTER* appliance.

Referenced from NETLAB+ Installation Guide - NetDevGroup.com

13. If a *Confirm Reboot* window pops up, click **Yes** to continue.
14. Confirm that the *VCENTER* appliance boots up correctly by watching the boot process through the console screen.

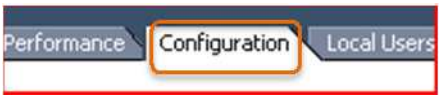
## 4.12 Automatic Startup for vCenter

In this section, *vCenter* will be configured to automatically start with the ESXi Management Server. This is important because if it is not set up correctly, if the *ESXi Management Server* powers off or reboots, the *vCenter Appliance* within the server will require a manual boot causing lost of connectivity between the NETLAB+ server and the VMware environment.

The following steps will help guide you in configuring automatic startup for *vCenter*:

1. Login to *vCenter* using the *vSphere Client*.
2. Click on the **ESXi** host in the left pane window.

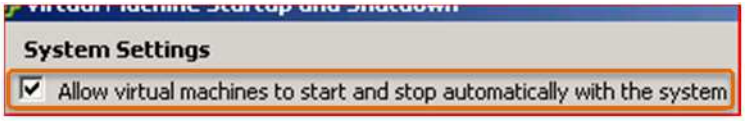
3. Click the **Configuration** tab at the top.



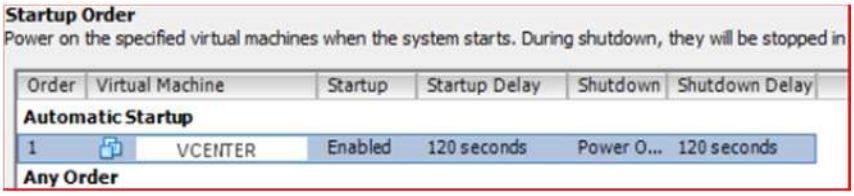
4. Under the *Software* section, click on **Virtual Machine Startup/Shutdown**.

5. Click on **Properties** in the upper right.

6. Click the checkbox next to **Allow virtual machines to start and stop automatically with the system**.




7. Make sure to select your **vCenter** VM in the list and click **Move Up** until it is under *Automatic Startup*.




Referenced from NETLAB+ Installation Guide - NetDevGroup.com

8. Click **OK**.

9. Close the *vSphere client*.

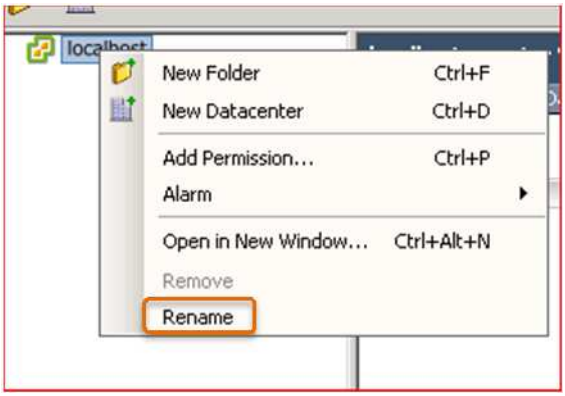
## 4.13 Datacenter Configuration

In this section of the guide, you will create a datacenter, add ESXi Host Servers, configure ESXi firewall to allow Remote PC Viewer sessions, and configure vSwitch.

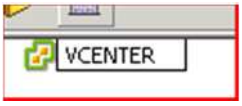
### 4.13.1 Creating NETLAB+ Datacenter in vCenter

The following step will help create a NETLAB+ datacenter on the *vCenter*:

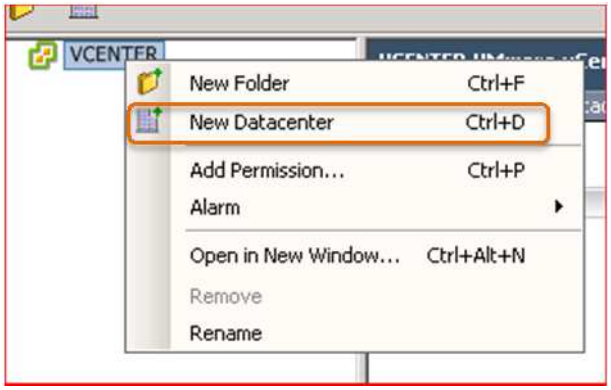
1. Using the *vSphere Client*, log into the *vCenter* using the IP address you set in Section 3.4.
2. Right-click the *vCenter* host, **localhost**, on the left and select **Rename**.




3. Set the hostname to **VCENTER** and press **Enter**.




4. Right-click on the **VCENTER** host and select **New Datacenter**.

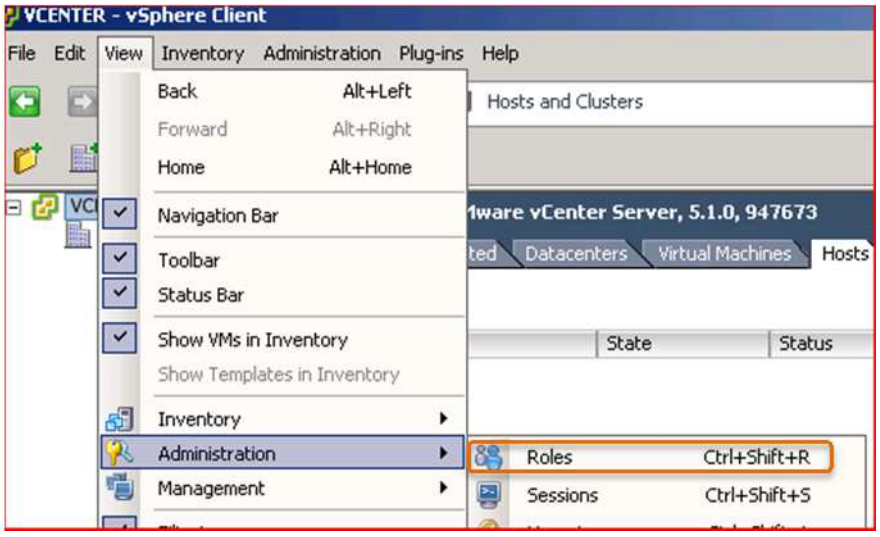


5. Set the name of the datacenter to **NETLAB** and press **Enter**.

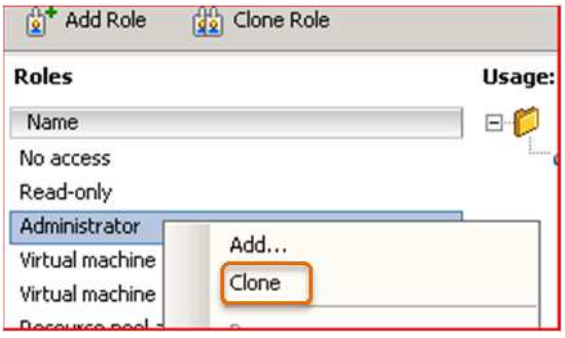
### 4.13.2 Creating a NETLAB+ Role in vCenter

The following steps will help create a NETLAB+ role in *vCenter* to map to the NETLAB+ user you created in Section 3.9:

1. Login to *vCenter* using the *vSphere Client*.
2. In the *vSphere Client*, click on **View > Administration > Roles** from the menu toolbar.

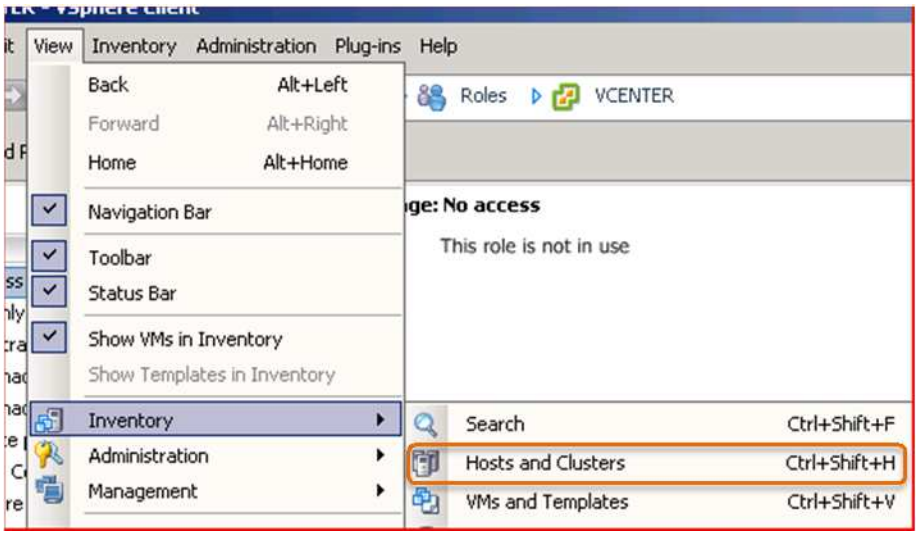



3. Right-click on **Administrator** under *Roles* and select **Clone**.

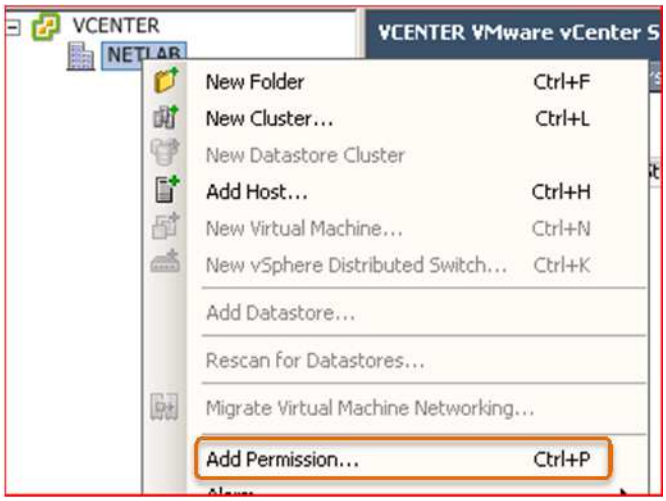


4. In the new role field, type **NETLAB** and press **Enter**.

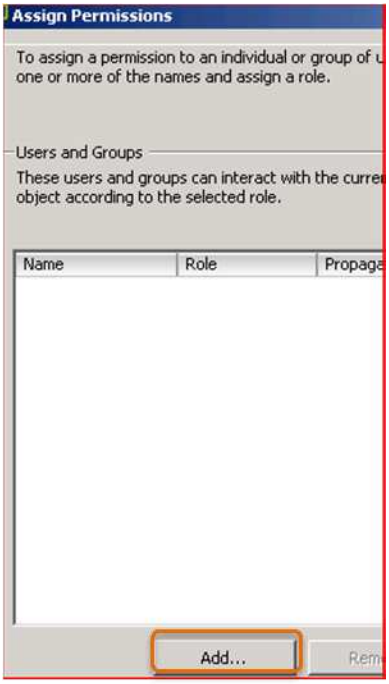
5. Click **View > Inventory > Hosts and Clusters** from the top menu toolbar.



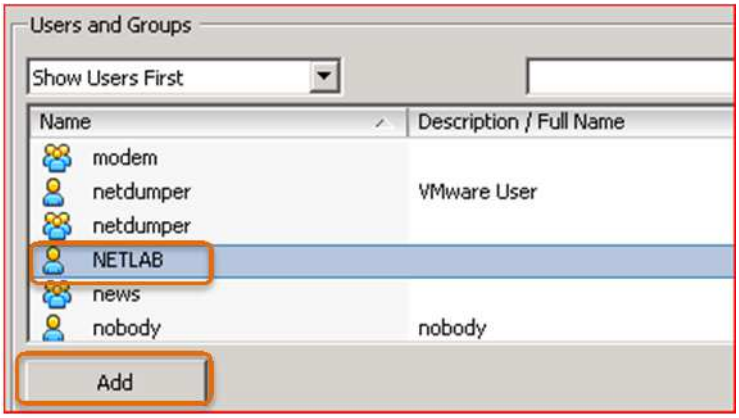

6. Right-click on **NETLAB** and select **Add Permission…**



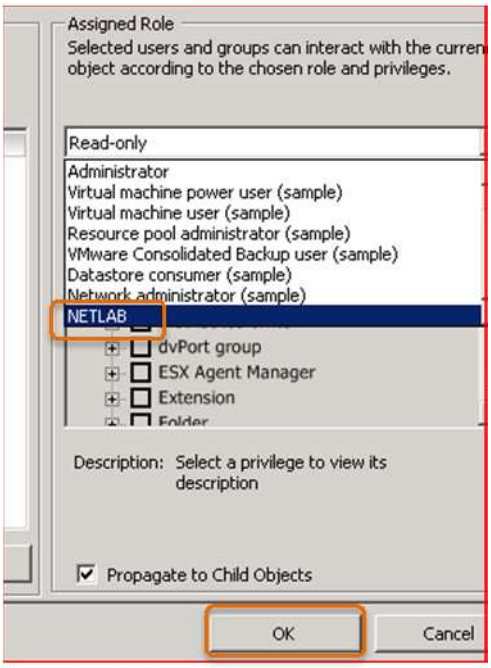
7. In the *Assign Permissions* window, click the **Add...** button.


Assign Permissions
To assign a permission to an individual or group of u
one or more of the names and assign a role.
Users and Groups
These users and groups can interact with the curre
object according to the selected role.
Name
Role
Propaga
Add...
Rem

8. In the user list, select the **NETLAB** account. Click **Add**, followed by **OK**.



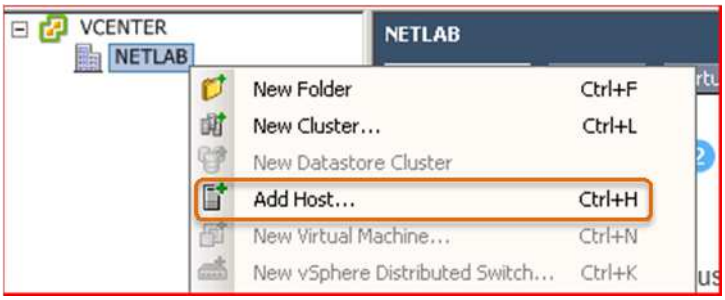
9. In the *Assign Permissions* window, from the drop down box in the *Assigned Role* area, select **NETLAB** and then **OK**.



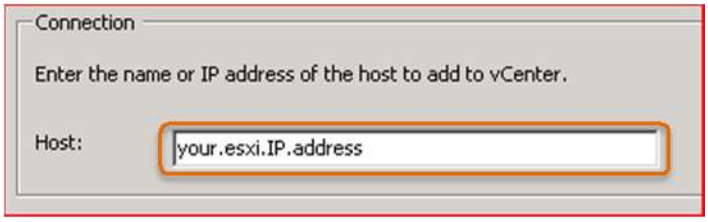

### 4.13.3 Adding ESXi Hosts to the NETLAB+ Datacenter

The following steps will help guide the process of adding *ESXi Host Servers* to the NETLAB+ datacenter (these host servers will be managed by your *vCenter*):

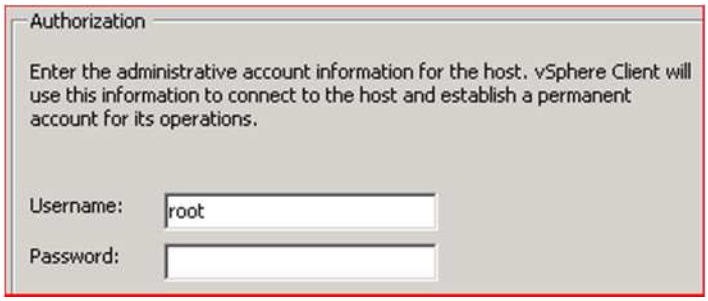
1. Login to *vCenter* using the *vSphere Client*.
2. Right-click on the **NETLAB** datacenter and select **Add Host**.



3. In the *Add Host* wizard, enter the IP address of the first ESXi host that you wish to add.




4. Enter the username **root** and password you have chosen when installing the ESXi software onto the host server.


Authorization
Enter the administrative account information for the host. vSphere Client will use this information to connect to the host and establish a permanent account for its operations.
Username:
root
Password:

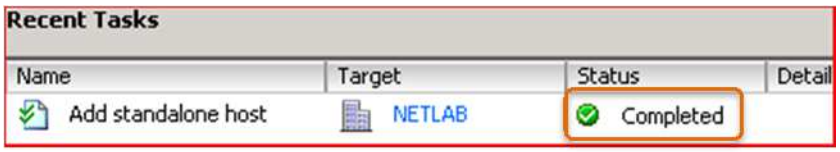
5. When prompted with a *Security Alert*, select **Yes** to add the host.

Security Alert
Unable to verify the authenticity of the specified host.
The SHA1 thumbprint of the certificate is:
29:CF:B9:C6:15:57:D2:CD:B9:24:B9:54:18:99:B3:5F:DC:B6:11:04
Do you wish to proceed with connecting anyway?
Choose "Yes" if you trust the host. The above information will be remembered until the host is removed from the inventory.
Choose "No" to abort connecting to the host at this time.
Yes
No

6. Review the information on the *Host Summary* page and click **Next**.

7. On the *Assign License* page, select radio button next to "*Assign a new license key to this host*" and select **Enter Key**.

8. Enter the key provided by the VMware IT Academy (http://communities.vmware.com/docs/DOC-18121). This key is to be used for your infrastructure equipment only.
9. On the *Lockdown mode* page, leave the default settings and click **Next**.
10. On the *Virtual Machine Location* page, be sure to select **NETLAB** and click **Next**.
11. On the *Ready to Complete* page, review the information and click **Finish**.
12. Click the **+** sign next to the *NETLAB datacenter* on the left and wait for the IP address of the host you entered to be added.
13. Review the *Recent Tasks* pane on the bottom right to make sure the task completes.



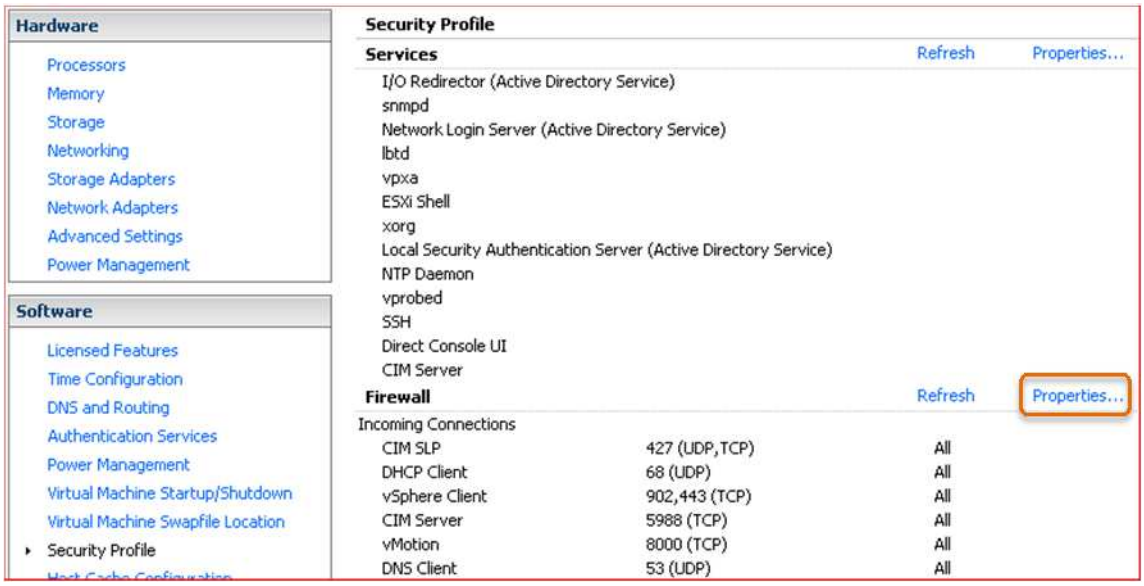

14. Repeat steps 1-11 from Section 3.13.3 to add any additional host servers.

### 4.13.4 Configuring ESXi Firewall to Allow Remote PC Viewer Sessions

The following steps will help guide the process of allowing specific port ranges in the ESXi firewall to allow *Remote PC Viewer* sessions to have access to the virtual machine console:

1. Login to *vCenter* using the *vSphere Client*.
2. Select the first **ESXi** host in the **Inventory** pane on the left side, when viewing the *vSphere Client*.
3. Click on the **Configuration** tab in the *main workspace* area.

4. Click on **Security Profile** in the *Software* box. Then click on the **Properties…** hyperlink next to the *Firewall* options to review the built-in ESXi firewall settings.




5. A *Firewall Properties* window will appear, scroll to the bottom of the list and place a checkmark next to **VM serial port connected over net…** Click **OK** to save settings.

6. It is important to repeat steps 1-4 of Section 3.13.4 for every *ESXi Host Server* that is being added to the infrastructure.

## 4.14 vSwitch Configuration

In this section, the focus is going to change to how vSwitches are configured on the ESXi Host Servers. A virtual switch is called a vSwitch on the physical *ESXi Host Server.* It bridges between physical networks, virtual machines, and the ESXi host kernel. It is important to note that each vSwitch is an internal Local Area Network (LAN) that is implemented entirely in software by the ESXi kernel.

The diagram below shows a visualization of how a vSwitch sits inside of an *ESXi Host Server* with a physical network interface card (NIC) attaching to a physical switch.

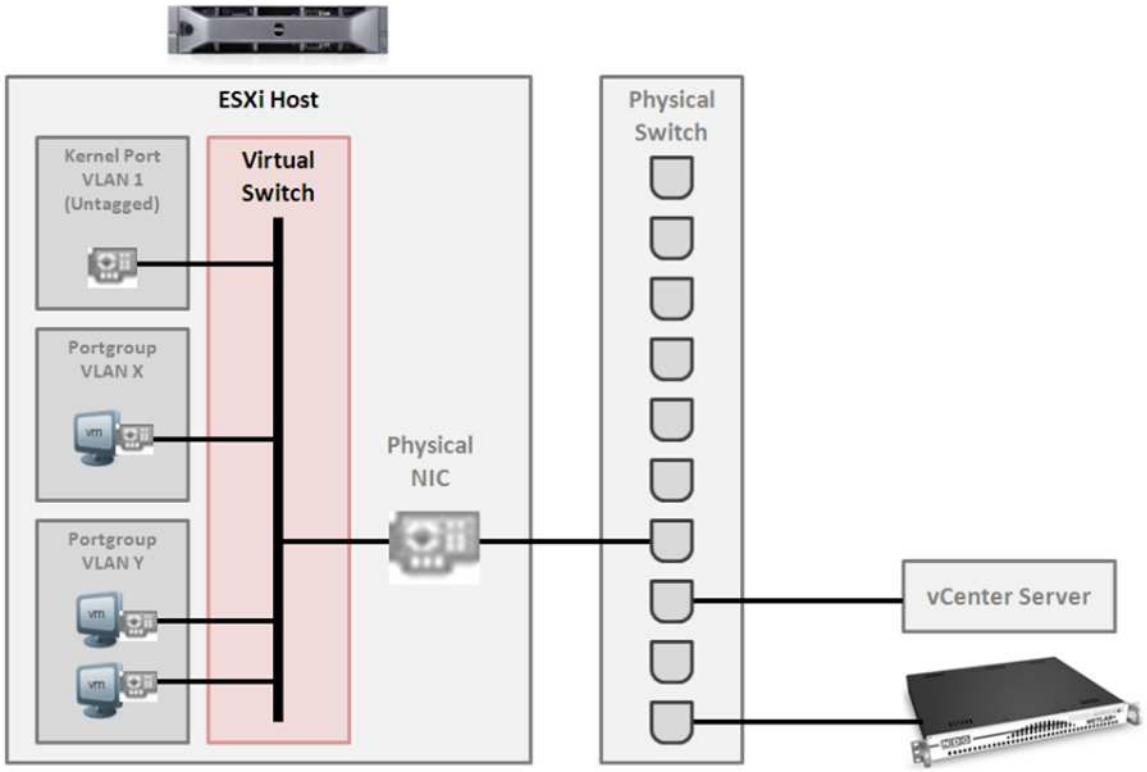



Diagram from Remote PC Guide Series – Volume 2 NetDevGroup.com

Depending on your infrastructure, your ESXi host(s) may have virtual switches used for either outside or inside connections. See the table below to see how a vSwitch in an ESXi host would be configured.

| Network Model | OUTSIDE vSwitch | INSIDE vSwitch |
|---|---|---|
| **Single-Homed** | vSwitch0 | n/a |
| **Dual-Homed** | vSwitch0 | vSwitch1 |

## 4.15 Verifying vSwitch0 Configuration

During the ESXi software installation, by default, vSwitch0 is automatically created. It is important to review and confirm that networking on vSwitch0 is properly configured.

The following steps will help review the configuration of vSwitch0:

1. Login to *vCenter* using the *vSphere Client*.

2. While in the *vSphere Client*, select an appropriate **ESXi Host Server** that has been added to the *vCenter*.
3. Once you have an ESXi host selected, select the **Configuration** tab in the *main workspace* area.

4. Click on the **Networking** hyperlink located under *Hardware*.

5. Make sure to select the **vSphere Standard Switch** button next to *View:*.

6. Here are the things that need to be reviewed for vSwitch0:
   a. vSwitch0 is bound to the correct physical NIC (vmnic).
   b. The physical NIC is connected with correct speed/duplex.
   c. The VMkernel port has the IP address you assigned when configuring the ESXi Host Server. The IP address should be a campus LAN address.
7. Repeat steps 1 through 6 if you have more than one *ESXi Host Server*.

## 4.16 Inside Network Configuration

This section will deal with inside networking. This section only applies to the Dual-Homed networking configuration that connects the *ESXi Host Server* to the inside network with real live equipment such as Cisco equipment used for labs.

The only type of traffic that flows across the ESXi inside network is remote PC traffic between virtual machines hosted on the ESXi itself and real equipment. VLANs 100 through 899 will be used automatically assigned here.

### 4.16.1 Creating vSwitch1 and Binding to a Physical NIC

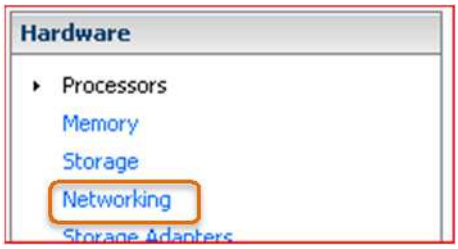
When utilizing a Dual-Homed network, an inside virtual switch (vSwitch1) must be created and bound to a physical NIC along with creating a VMkernel port for management traffic.

The following steps will help configure vSwitch1:

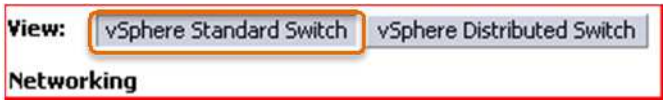
1. Login to *vCenter* using the *vSphere Client*.
2. Navigate to **Home > Inventory > Hosts and Clusters**.

3. Click on an **ESXi Host Server** to configure on the left side.
4. Click on the **Configuration** tab in the *main workspace* area.

5. Click on the **Networking** hyperlink located under *Hardware*.



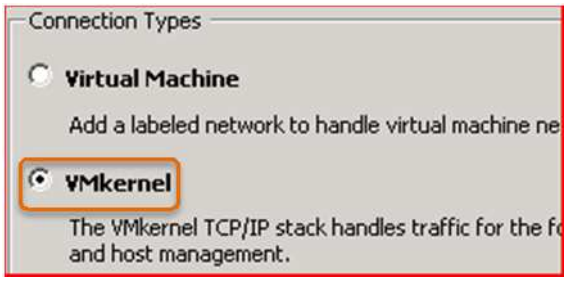

6. Select the **vSphere Standard Switch** button next to View: if not already selected.



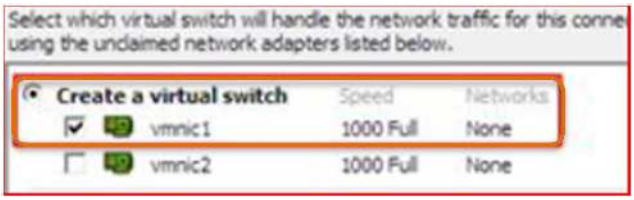

7. Select the **Add Networking** hyperlink.

8. An *Add Network Wizard* window will be displayed.

9. Make sure to select the radio button next to **VMkernel** to allow the *ESXi Host Server* kernel to communicate with the inside network. Click **Next**.

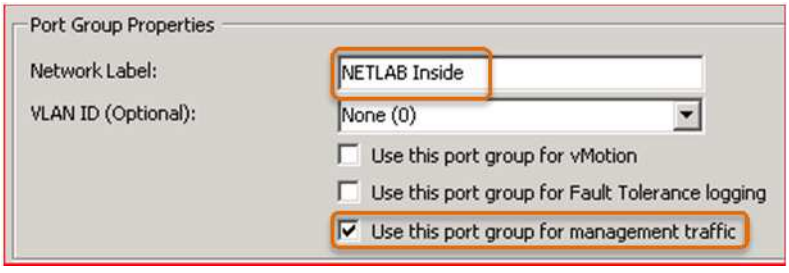

Connection Types
Virtual Machine
Add a labeled network to handle virtual machine ne
VMkernel
The VMkernel TCP/IP stack handles traffic for the fo
and host management.

10. Select the radio button next to **Create a virtual switch**. The new switch will be named vSwitch1.




Referenced from NETLAB+ Remote PC Guide Series - NetDevGroup.com

11. Now select the physical NIC that will connect vSwitch1 to the control switch. NDG recommends using **vmnic1** for inside connections (vmnic0 should already be used to connect to the outside network).
12. On the *VMkernel – Connection Settings* page, enter the following port group properties:
    a. Network Label: **NETLAB Inside**
    b. VLAN ID: **None (0)**
    c. Check the option: **Use this port group for management traffic**


Port Group Properties
Network Label:
NETLAB Inside
VLAN ID (Optional):
None (0)
Use this port group for vMotion
Use this port group for Fault Tolerance logging
Use this port group for management traffic

13. Click **Next**.
14. On the *VMkernel – IP Connection Settings* page, enter a unique IP address and subnet mask from the following table. NDG recommends assigning inside ESXi host interfaces with an IP address between **169.254.0.241 - .249**.

| Inside Interface | IP Address | Subnet Mask |
|---|---|---|
| **ESXi Server 1 Inside** | 169.254.0.241 | 255.255.255.0 |
| **ESXi Server 2 Inside** | 169.254.0.242 | 255.255.255.0 |
| **ESXi Server 3 Inside** | 169.254.0.243 | 255.255.255.0 |
| **ESXi Server 4 Inside** | 169.254.0.244 | 255.255.255.0 |
| **ESXi Server 5 Inside** | 169.254.0.245 | 255.255.255.0 |
| **ESXi Server 6 Inside** | 169.254.0.246 | 255.255.255.0 |
| **ESXi Server 7 Inside** | 169.254.0.247 | 255.255.255.0 |

15. No changes need to be made to the *VMkernel Default Gateway* as this should be already set to the default gateway on your campus LAN.
16. Click **Next** to continue.
17. Confirm that vSwitch1 is displayed properly under the networking portion for the *ESXi Host Server*.
    a. *VMkernel Port* (vmk1) has correct IP address.
    b. *vSwitch1* is bound to the physical adapter *vmnic1*.
    c. Physical adapter is up with speed and duplex configurations appearing properly.
18. Repeat steps 1 through 17 if you have more than one *ESXi Host Server* supporting real equipment.

### 4.16.2 Increasing the Inside vSwitch Port Count

By default, a vSwitch is provisioned with 56 virtual ports. What this means is that 56 virtual network adapters can be connected to the virtual switch. When using a NETLAB+ AE setup, this would be sufficient enough for the inside vSwitch. However, for large NETLAB+ PE setups or systems with custom real equipment pods, the value of virtual ports may need to be increased to accommodate more virtual machine connections to the inside vSwitch.

In order to calculate the number of inside vSwitch ports required on a particular *ESXi Host Server*, add up the number of virtual machines in real equipment pods that are assigned to the host. This is assuming one connection per VM.

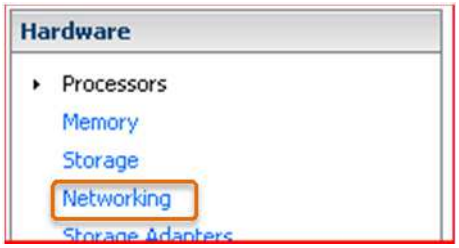
For example, if the number exceeds 50, you should select the next highest port count setting which would be 120. The value could be higher than 120 for special cases which is fine but the value should be set to the lowest possible setting that provides enough ports for every counted VM connecting to the inside vSwitch of a particular *ESXi Host Server*.

The following steps will be used to increase the number of virtual ports:

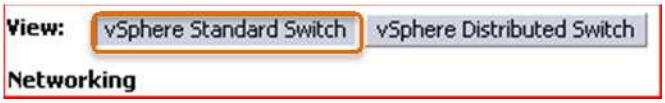
1. Login to *vCenter* using the *vSphere Client*.
2. Navigate to **Home > Inventory > Hosts and Clusters**.

3. Select the **ESXi Host Server** you want to configure.
4. Click on the **Configuration** tab in the *main workspace* area.

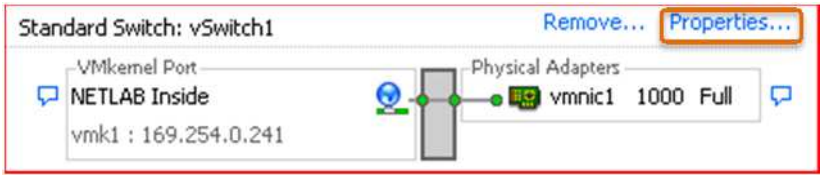
5. Click on **Networking** listed under *Hardware*.



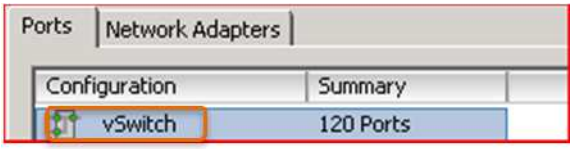

6. Click on the **vSphere Standard Switch** button if not already selected.




7. Click **Properties** on the *INSIDE vSwitch*. Remember, this vSwitch is the one that is connected to the control switch.

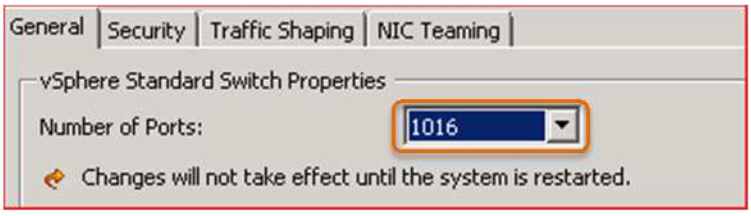


8. Click on the **vSwitch** listed on the left side of the *Properties* window.




9. Click the **Edit** button.

10. Increase the number of ports here, but remember to choose the lowest value that will accommodate the total number of inside virtual machines you accounted for. (For example, lets assume you have planned a total of 900 VMs from all of the pod deployments. Rounded up for some head room, the closest value would be 1016.)




11. Click **OK**.
12. Right-click on the **ESXi Host Server** in the left tree view. Select **Reboot**.

13. Repeat steps 1 through 12 if you have more than one *ESXi Host Server* supporting real equipment.

### 4.16.3 Creating a SAFETY NET

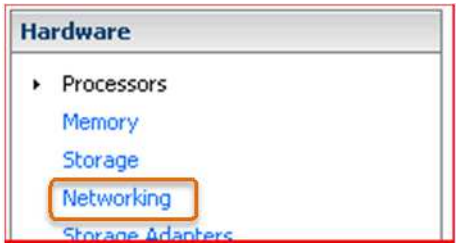
In this section, a safe staging network will be created called "*SAFETY NET*". The purpose of the safe staging network is to prevent any of the virtual machines from posing a security risk to your campus LAN or interfere with other pods until they are relocated to their final networks via the automatic networking done by NETLAB+. It consists of a virtual switch and a port group that is not connected to any other network, kind of like its own isolated network that acts as a sandbox environment.

> *Important Note: The ESXi Host Server must be restarted in order for changes to take effect. Make sure there are no active NETLAB+ reservations or virtual machines running on the host.*

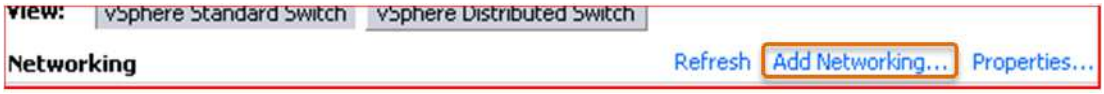
The following steps will help create a *SAFETY NET*:

1. Login in *vCenter* using the *vSphere Client*.
2. Select the appropriate **ESXi Host Server** in the *Inventory* pane on the left side.
3. Click the **Configuration** tab in the *main workspace* area.

4. In the *Hardware* box, click on **Networking**.

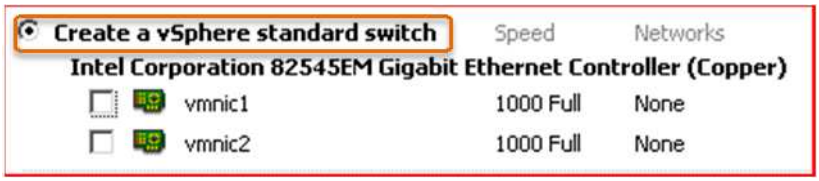



5. Then click on the **Add Networking...** hyperlink to create a new virtual switch.




6. On the *Connection Type* page, select **Virtual Machine**. Click **Next**.

7. On the *Network Access* page, make sure to select **Create a vSphere standard switch**. Make sure that no physical adapters are selected.




8. Click **Next** to continue.
9. On the *Connection Settings* page, enter **SAFETY NET** in the *Network Label* field. Click **Next**.

10. On the *Summary* page, review the information. Click **Next**.
11. Repeat steps 1 through 9 if you have more than one *ESXi Host Server*.

# 5 Configuring NETLAB+

## 5.1 Background

This section of the guide will help attach the virtual machine infrastructure that was created in Section 3 to NETLAB+. NETLAB+ maintains a database called the Virtual Machine Inventory. This inventory is able to map the remote PCs and virtual machines in one or more vSphere datacenters.

## 5.2 Register a Virtual Datacenter with NETLAB+

This section of the guide will provide directions on how to add a *vCenter* datacenter created during the virtual machine infrastructure setup to NETLAB+.

The following steps will help you register a virtual datacenter in NETLAB+:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Virtual Machine Infrastructure** icon.

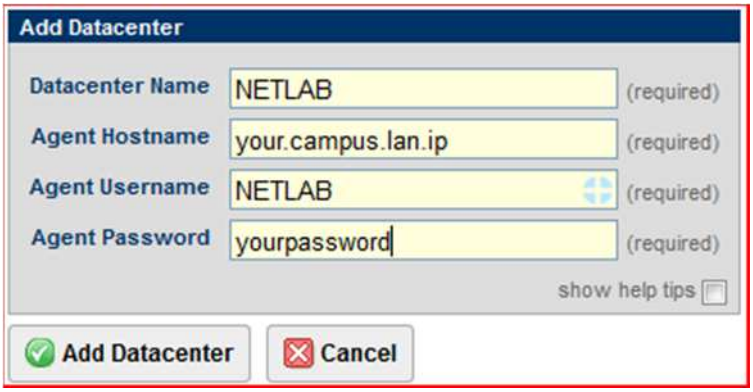
3. Click on **Virtual Datacenters and Management Agents**.

Virtual Datacenters and Management Agents
Define the virtual datacenters that contain your virtual machines and managment agents (i.e. vCenter) used to broker NETLAB+ automation requests.

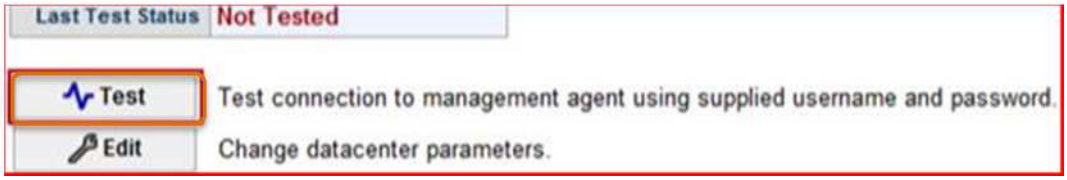
4. Click on **Add Datacenter**.

5. Fill in the required fields for the datacenter that has been setup using the *vSphere Client*.
    a. **Datacenter Name**: This will be **NETLAB** if you used the recommended name provided in this guide when adding a datacenter in *vCenter*.

b. **Agent Hostname**: This value is set to be the campus LAN IP address assigned to your *vCenter* server.
c. **Agent Username**: This is the username that was created when configuring the *vCenter Server Appliance*. If you followed the recommended setup, this should be **NETLAB**. This username will be used when NETLAB+ connects to *vCenter*.
d. **Agent Password**: This is the password that was created when configuring the *vCenter Server Appliance*. For example, it is the password used for the account *NETLAB*.




6. Click **Add Datacenter** to complete the registration.
7. Select **OK** to continue.
8. Click on **Test** to verify that NETLAB+ can connect to the *vCenter* server using the settings you provided.




Referenced from NETLAB+ Remote PC Guide Series – Volume 3 NetDevGroup.com

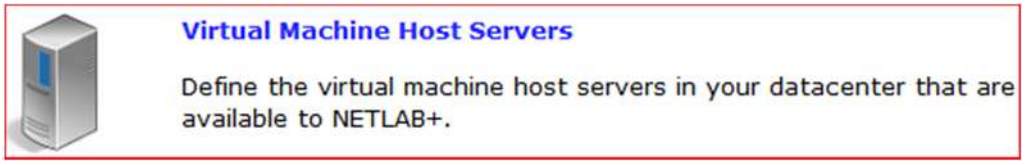
9. Click **OK** to continue.
10. Click **Exit** to return to the datacenter list.
11. Repeat steps 1 through 9 if you are adding more than one datacenter to NETLAB+.
12. Click **Exit** to leave the datacenter list.

## 5.3 Adding ESXi Host(s) in NETLAB+

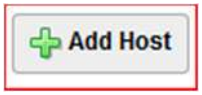
This section will help guide you through the process of adding *ESXi Host Servers* to NETLAB+. The following steps will help you add an ESXi host to NETLAB+:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Virtual Machine Infrastructure** icon.

3. Click on **Virtual Machine Host Servers**.




4. Click on the **Add Host** button.

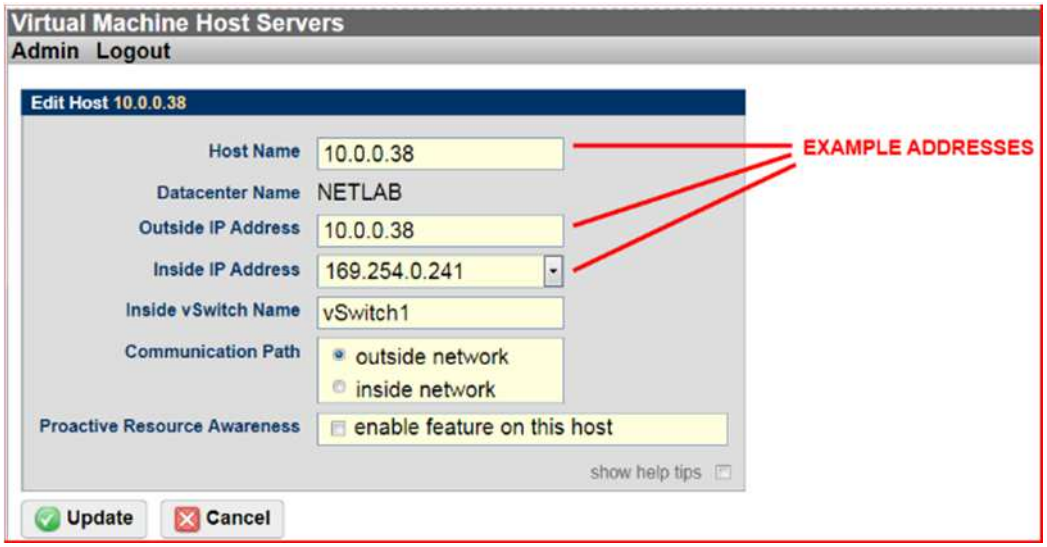



5. It is important to know that NETLAB+ scans the datacenter to discover *ESXi Host Servers*. The hosts that have not been registered in NETLAB+ are displayed. Select the host that you wish to add by clicking on the **host name** in the list.
6. Once a host is selected, values will have to be filled based on the networking model you have chosen. The table below shows the typical settings used:

| Networking model | Outside Address | Inside Address | Inside vSwitch | Communication Path |
|---|---|---|---|---|
| **Single-Homed** | Campus LAN IP Address | Not set | n/a | Outside |
| **Dual-Homed** | Campus LAN IP Address | 169.254.0.X | vSwitch1 | Outside |

   a. **Host Name**: This is the IP address or fully qualified domain name of the *ESXi* host. This should be the same value entered when the host was added to *vCenter*.
   b. **Outside IP Address**: The IP address of the ESXi outside interface.
   c. **Inside IP Address**: The IP address of the ESXi inside interface. Use the "not set" option for when using a single-homed networking model.

d. **Communication Path**: This will always be set to outside network as inside network was for compatibility with previous networking models.
e. **Inside vSwitch Name**: This is the name of the virtual switch within the *ESXi Host Server* that connects to the control switch. Typically, this will be vSwitch1 for dual-homed networking models. This setting may be left blank if using a single-homed networking model (the vSwitch name is case sensitive).




Referenced from NETLAB+ Remote PC Guide Series – Volume 3 NetDevGroup.com

13. Click **OK** to confirm the host has been added.
14. Click **Exit** to return to the host list.
15. Repeat steps 1 through 14 for any additional *ESXi Host Servers* that may need to be added.

## 5.4 Proactive Resource Awareness

Proactive Resource Awareness (PRA) allows time-share between virtualization servers using the NETLAB+ scheduler. Using PRA, you may set 3 different limits:

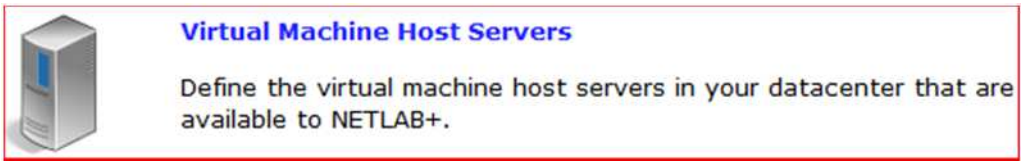
- Total number of active VMs
- Active number of vCPUs
- Active maximum memory usage

The purpose of PRA is to allow the administrators control the available resources.

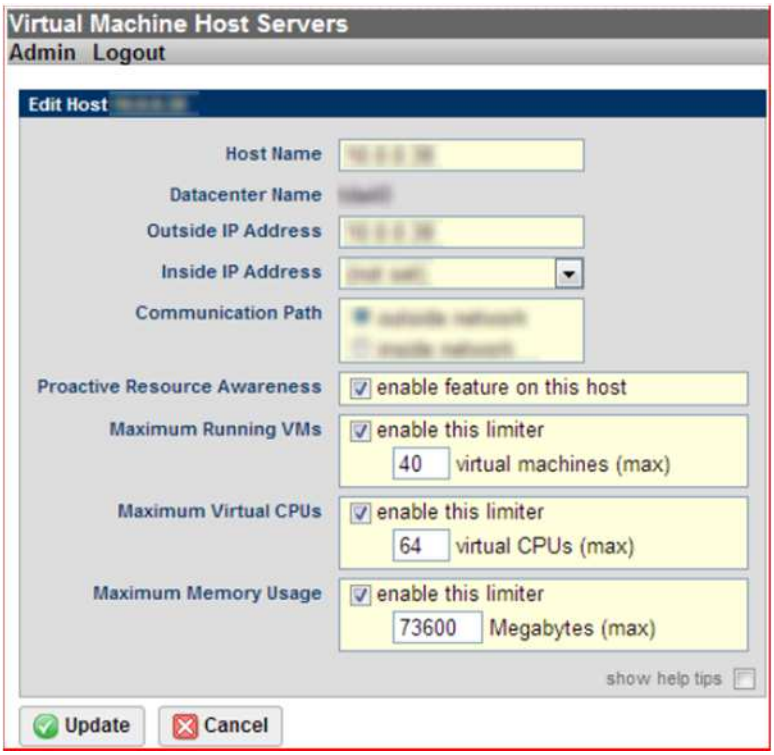
The following steps will help guide you through setting up PRA:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Virtual Machine Infrastructure** icon.

3. Click on **Virtual Machine Host Servers**.




4. Select an **ESXi Host Server** to edit its settings.
5. When viewing the host settings, the PRA fields can be found towards the bottom:
    a. **Proactive Resource Awareness**: Place a checkmark here to enable PRA on the host.
    b. **Maximum Running VMs**: Place a checkmark here to enable the VM limiter. Set the number of virtual machines that you wish to be the maximum on the host.
    c. **Maximum Virtual CPUs**: Place a checkmark here to enable the virtual CPU limiter. Placing a value here will determine how many virtual CPUs can be running at one time.
    d. **Maximum Memory Usage**: Place a checkmark here to enable the memory limiter. This will place a limit on how much memory can be used at one time for the host. NDG recommends taking the total amount of RAM and subtracting 8GB or 8192MB.




Referenced from NETLAB+ Remote PC Guide Series – Volume 3 NetDevGroup.com

## 5.5 Local System ID for Multiple NETLAB+ Systems

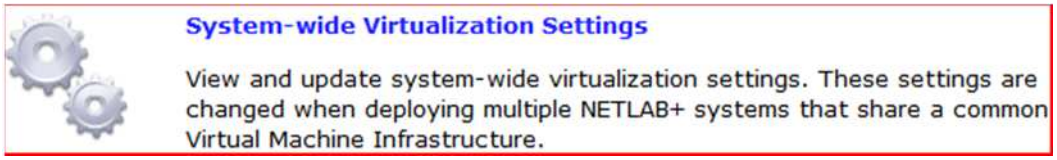
It is important to note that if more than one NETLAB+ system is being used or if they access a common VMware vCenter and/or ESXi Host Servers, it is necessary to set the System Local ID of your NETLAB+ systems so that each NETLAB+ system is uniquely identified.

If you are using only one NETLAB+ appliance, then using the default value "001" is sufficient.

The following steps will help guide you in updating the System Local ID:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Virtual Machine Infrastructure** icon.

3. Click on **System-Wide Virtualization Settings**.


System-wide Virtualization Settings
View and update system-wide virtualization settings. These settings are changed when deploying multiple NETLAB+ systems that share a common Virtual Machine Infrastructure.

4. Change the value accordingly. Click **OK** when finished.

# 6 Administrator Guide

## 6.1 Background

When operating within the NETLAB+ web interface, there are many tools that the administrator can use. NETLAB+ is able to offer an easy to use platform which requires no UNIX knowledge from the administrator.

When following this section, everything will be done using the NETLAB+ web interface. The tasks performed using the web-based interface include viewing logs and alerts, performing system maintenance, management of administrator and instructor accounts, and equipment configuration.

## 6.2 Editing the Administrator Profile

It is a good practice to edit the contact information for both technical and business contacts. This helps out the NDG support team when they are trying to reach out to the appropriate person when a problem rises.

A NETLAB+ administrator can easily change their contact information by following the steps below:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Administrator Profile** icon.

3. Click on **Update Contact Info**.

4. Make appropriate changes and then click the **Update Contact Info** button to shave changes.

In the same interface (Administrator Profile), you are able to change the password of the administrator account by clicking the Change Admin Password.

## 6.3 Managing Communities

A community is a selective group that includes instructors, students, and classes. This only allows instructors to manage students and classes within their own community, unless granted system-wide privileges by the administrator.

Multiple communities can be made to facilitate the sharing of a NETLAB+ system among several different groups such as schools, institutions, academies, etc..

For example, when using a NETLAB+ AE, each academy using your system should be defined as a community. If the system is being used by a single academy, only the default community should be used.

Having multiple communities is optional, but it is important to remember that each instructor, student, and class can belong to only one community.

### 6.3.1 Adding Communities

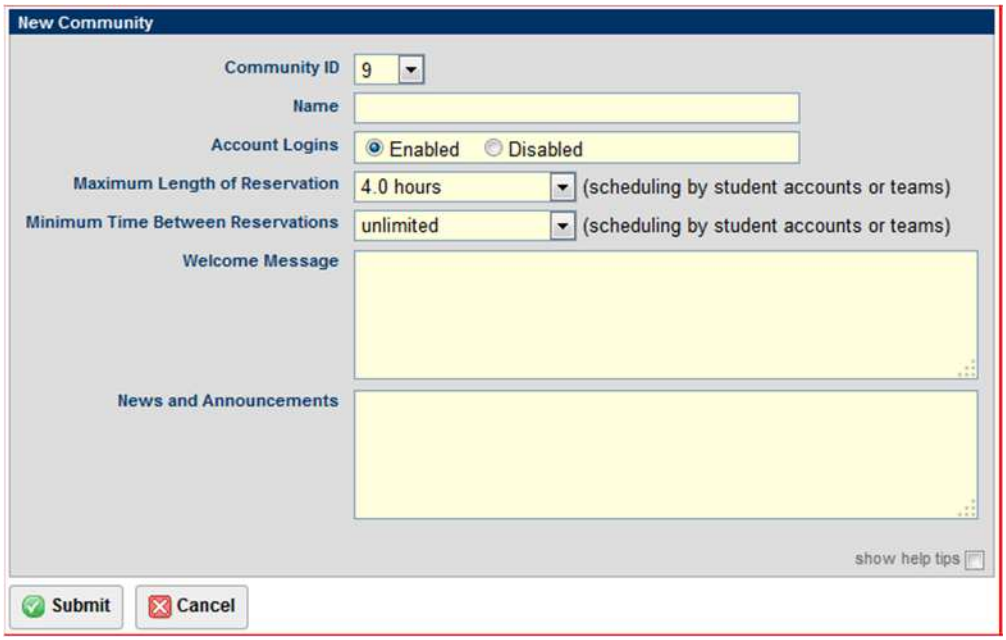
The following steps will help guide in when adding new communities (only the administrator may add new communities):

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Communities** icon.

3. Click on **Add Community**.

4. Enter the information regarding to your new community:
    a. **Community ID**: This value determines the order in which this community is displayed in the community list.
    b. **Name**: A name for the community.
    c. **Account Logins**: Enable or disable logins done by the users in this community.

d. **Maximum Length of Reservations**: This will be the posted maximum length of time a reservation can be scheduled by an individual student or team. This does not however affect instructors.
e. **Minimum Time Between Reservations**: This is the minimum time that must elapse before an individual student or team in a class can make another reservation after one has just passed. This does not affect the instructors.
f. **Welcome Message**: This will appear at the top of the MyNETLAB page for all users belonging to the community.
g. **News and Announcements**: This information will appear on top of the MyNETLAB page, below the welcome message for all users belonging to the community.




5. Once all information is entered, go ahead and click **OK** to add the community.

## 6.4 Managing Classes

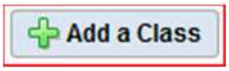
Within the NETLAB+ web interface, administrators are able to manage classes and rosters easily. This is a great tool which helps map class rosters with real classes that students are involved with.

### 6.4.1 Adding Classes

The following steps will help guide the process of adding classes:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Classes** icon.

3. Select a community that you wish to add a class to. If no communities are made, the default community may be used.
4. To add a class, click on the **Add a Class** button.




5. Edit the form fields:
    a. **Class Name**: The name of the class must be unique from any other classes.
    b. **Lead instructor(s)**: Add instructors who wish to be the trainers for the class. Only lead instructors can schedule instructor-led lab reservations for a class. Lead instructors can also join any student or team reservations in progress that are associated with the class.
    c. **Global Labs**: Select the appropriate lab exercises and content that can be accessed by users in the class roster. This also affects the pod types that users can access. It is important to note that this decision needs to be closely followed and observed as students will be given access to the curriculum materials of whichever labs are checked.
    d. **Private Labs**: If you have created lab designs using the Lab Designer, they will be available for selection.
    e. **Starting Date**: This is optional for when designating a start date for the class. Users will be unable to reserve pod sessions before the selected date.

f. **Ending Date**: This is optional for when designating an end date for the class. Users will be unable to reserve pod sessions after the selected date.
g. **Self Study Lab Access**: If Individuals is selected, individual users in the class roster can schedule lab reservations. If Teams is selected, users in the class roster can schedule the pods for use as a team.
h. **Predetermined Lab Time Limits**:
    i. Enforce lab author's time limits (if any): If the author of a lab that is being used in the class has specified a time limit, this will give a time frame for when the lab should be completed by a student.
    ii. Do not enforce lab author's time limits: This option will disregard any time limits set by lab authors.
i. **Preferred Maximum Length of Reservation**: This option will help set the maximum length of a reservation (individual or team).
j. **Preferred Minimum Time Between Reservations**: This option sets the minimum length of time that an individual student or team must wait before making another reservation after a lab has been initiated. The default value is set to no limit which means that a student or team will be able to make unlimited reservations.
k. **Console Password**: This option applies to Cisco courses only. This password assumes the position of "line con 0" for all device consoles. When NETLAB+ performs an automated operation, it will try this password to gain access to the console. Some automated operations may abort if the device's console is not set to this value.
l. **Enable Password**: This option applies to Cisco courses only. This password assumes the position of privileged exec mode. When NETLAB+ performs an automated operation, it will try this password to gain access to privileged exec mode. Some automated operations may abort is the device's enable password is not set to this value.
m. **E-mail Configs/Logs**: This option applies to Cisco courses only. Once a reservation is completed, a copy of the configuration files may be automatically sent to lead-instructors.
n. **Retain Configs/Logs**: This option applies to Cisco courses only. Once a reservation is completed, a copy of the final configuration files and session logs can be saved into the NETLAB+ archive. This will however consume disk space as it will increase the size of backups.
o. **Instructor-led Reservations**: If this option is checked, NETLAB+ will save configuration files and session logs from instructor-led class reservations.
p. **Individual or Team Reservations**: If this option is checked, NETLAB+ will save configuration files and session logs from student or team reservations.
q. **Retention Period**: This option will specify how long you want NETLAB+ to retain configuration files and session logs in its archive bin for the class.

6. Once the form fields are populated, select **OK** to continue.

7. On the next page, you will be presented with two options; "**Choose Lead Instructors**" or "**Exit**". If you choose to add instructors, you then will have the option to add learners to the class; however you may also choose to add learners to the roster at a later time.

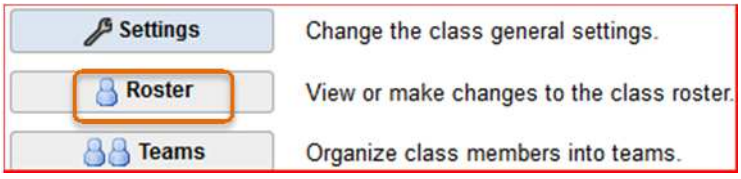
### 6.4.2 Adding Learners to the Class Roster

A class roster is referred to as a list of users that belong to a specified class. The list of users can include students and instructors. In NETLAB+ a class may contain one or more lead instructors who act as trainers. All the other users who are not considered as "leads" are learners.

The following steps will help guide you in adding learners to a specified class:

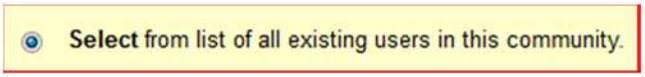
1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Classes** icon.

3. Select the associated community that you assigned the class to. If no communities have been made, click on **default**.
4. Here you will be presented with a list of classes. Select the class you wish to add learners to.
5. Click on the **Roster** button.

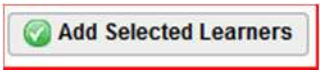



6. A list of learners assigned to the class will be displayed, or a message stating that no learners have yet been added to the class. Select **Add Learners**.

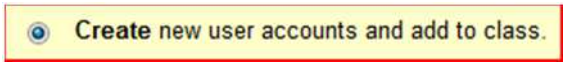
7. You will be presented with three options:
    a. The **Select** Method:
        i. The first method, *Select*, will allow you to select learners from an existing list of users in the community that the class is assigned to.



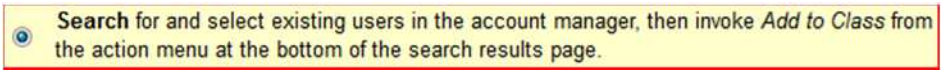

        ii. You will be selecting learners from accounts that already exist.
        iii. Place a **check mark** in the *Select* column to add learners to the class.
        iv. Click the **Add Selected Learners** button to add the learners to the class roster.




    b. The **Create** Method:
        i. The second method, *Create*, will allow you to create new accounts associated with each new learner you are adding to the class.




        ii. This option is used when you need to add learners to a class and have not yet set up accounts for them.
        iii. Enter the new account information for each user when presented with the *Enter New Account Information* screen.
    c. The **Search** Method:
        i. The third method, *Search*, will allow you to select existing users in the account manager and then invoke *Add to Class* from the action menu at the bottom of the search results page.


Search for and select existing users in the account manager, then invoke Add to Class from the action menu at the bottom of the search results page.

        ii. This option is ideally used when you will be selecting learners for which accounts already exist.
        iii. The search results display all of the student accounts in the community. Select the students you wish to add to the roster by placing a **check mark** in the *Select* column. Make sure **Add to Class Roster** is selected in the drop down box next to "*Perform Action on Selected Accounts*" and then click **Go**.

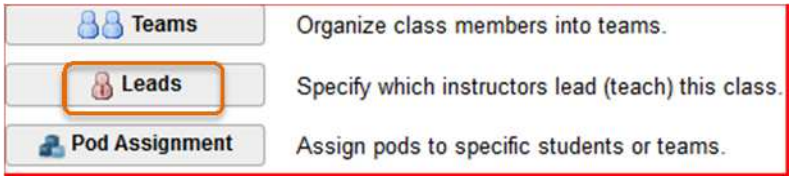
### 6.4.3 Adding Lead Instructors to a Class

For each active class that is made, a lead instructor should be defined. It is important to know that the lead instructor has the option to participate in any lab reservations associated within its class.

The following steps will help guide the process of adding lead instructors to a class:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Classes** icon.

3. Select the associated community that you assigned the class to. If no communities have been made, click on **default**.
4. Here you will be presented with a list of classes. Select the class you wish to add learners to.
5. Click on the **Leads** button.




6. All instructor accounts will be displayed. Select the instructors that you wish to make as leads for the class by placing a **check mark** next to each *user ID* under the *Select* column.
7. Click **OK** when finished.

## 6.5 Managing Accounts

NETLAB+ provides an easy to use manage accounts function that can be used to create, delete, and modify account information for both student and instructor accounts. A student account should be created for each individual student so that they have their own accounts to use to participate in labs.

As an administrator for NETLAB+, you may manage accounts for any community. You may also allow instructors to manage accounts for all communities by granting them system-wide privileges.

### 6.5.1 Adding Accounts

To add instructor or student accounts to the NETLAB+ system, follow the steps below:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Accounts** icon.

3. Click on the drop down menu next to *Community* to select a community where you would like to add an account to. If you have no communities set up, choose the default.
4. Select the **Add Accounts** button to display the add accounts screen.

5. Assign an initial (temporary) password to the accounts. The users will be required to change this password during their initial logon.
    a. Password must meet the following requirements:
        - Not found in the dictionary and not too simple
        - Between 7 and 16 characters
        - Contain both numbers and letters
6. Specify account information for each user account:
    **a.** **User ID**: This will be the user ID used for logging into the NETLAB+ system. May contain up to 16 ASCII alphanumeric characters and the underscore "_" character. Every user ID must be unique, no duplicates will be allowed. **User ID is case sensitive.**
    b. **Name**: The name of the user. Full name can be used here.
    c. **Type**: Specify whether the account is either a student or an instructor.

d. **E-mail Address** (optional): This is optional, account users will be prompted to add/update their email address and time zone information when they log into NETLAB+ for the first time.

7. Select the **Submit** button to add the new account(s) to the system.

### 6.5.2 Modifying Instructor Privileges

As the NETLAB+ administrator, you may edit information for any instructor or student account in any community. If you have multiple communities, you may wish to grant system-wide privileges to an instructor to allow the instructor to act as a system leader. It allows the instructor to manage accounts and classes in any community without accessing the administrator account.

Instructors with community-wide privileges act as a community leaders. They can manage accounts and classes within their own community.

Instructor with normal privileges (default) will only be able to manage their own student accounts and classes.

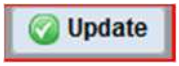
The following steps will help guide the process of editing instructor or student accounts:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Accounts** icon.

3. Click on the drop down box next to *Community* to select a community that the user account resides in. If you are unsure which community, leave the value to "**all**".
4. Next to "*Show*", you may filter what kind of user account you are searching for.
5. Once ready, click on the **Search** button.
6. Based on alphabetical order, click on the user ID of the account you wish to modify.
7. Here you will have the option to either; edit, delete, or reset the password for the account.

8. Click on the **Edit** button.

9. Make appropriate changes. Click **Update** to save changes.



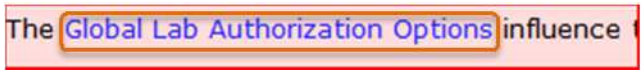

## 6.6 Managing Global Lab Authorization Options

It is important to note that global lab designs are authorized per community. This option is used to give access to the lab curriculum based on each community.

The following steps will help manage the global labs preferences:

1. Login to the NETLAB+ system using an administrator account.
2. Select the **Manage Installed Labs** icon.

3. Click on the **Global Lab Authorization Options** link or button.

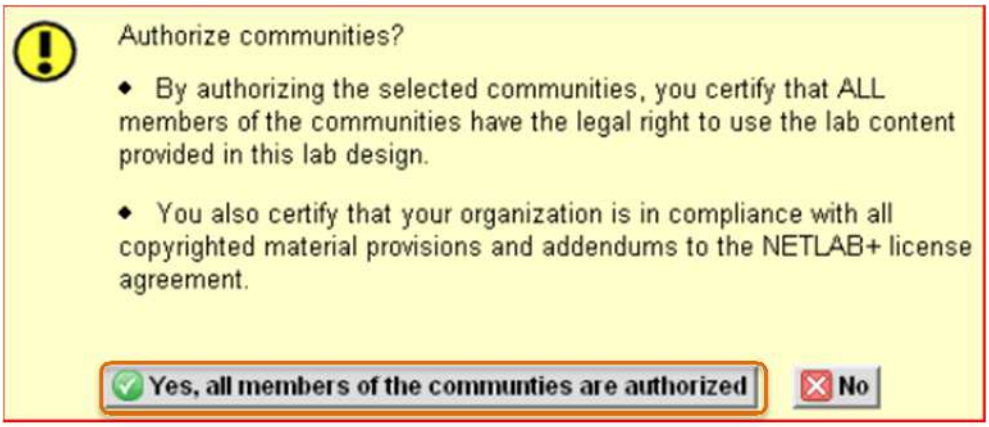


4. Select the appropriate preference for global lab authorization.
    a. **All**: When a new community is created, all existing global lab designs are automatically authorized to be used by the entire community. This will make it so that all newly made communities are authorized.

b. **Default**: When a new community is made, existing global lab designs must be manually authorized for the new community.
c. **Manual**: When a new community is made, existing global lab designs must be manually authorized for the new community. For all communities, the administrator must authorize access to allow the communities to access the new global lab designs.

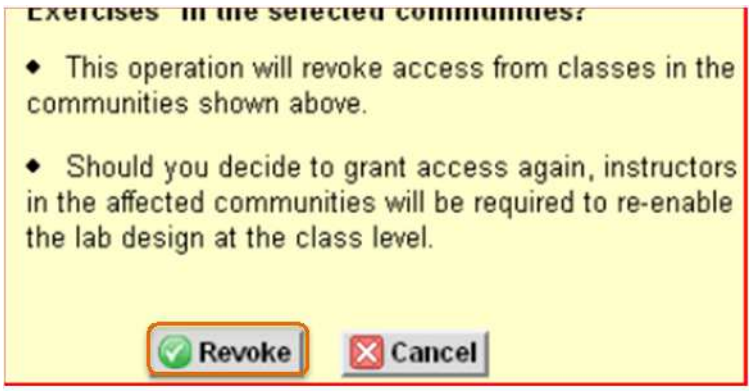
5. Select the name of a global lab design to view a list of communities that are currently authorized to access the lab design.
6. On the details page, view the *Authorized Communities* entries to see the current list of communities that have been authorized to use the lab design.
7. Select any community by placing a **check mark** next to the communities listed under the *Select* column. Based on your selection you will be able to either authorize or revoke.
8. Select the **Authorize Selected** button when you are ready to authorize.

a. If presented with a verification screen to authorize the selected, select **Yes** to confirm.


Authorize communities?
By authorizing the selected communities, you certify that ALL members of the communities have the legal right to use the lab content provided in this lab design.
You also certify that your organization is in compliance with all copyrighted material provisions and addendums to the NETLAB+ license agreement.
Yes, all members of the communities are authorized
No

Referenced from NETLAB+ Administrator Guide - NetDevGroup.com

9. Select the **Revoke Selected** button if you decide to revoke authorizations.
   a. If presented with a verification screen to revoke the selected, select **Revoke** to confirm.


Exercises" in the selected communities?
This operation will revoke access from classes in the communities shown above.
Should you decide to grant access again, instructors in the affected communities will be required to re-enable the lab design at the class level.
Revoke
Cancel

Referenced from NETLAB+ Administrator Guide - NetDevGroup.com

## 6.7 Equipment Pods

The equipment pods contain the lab devices and remote PC(s) that are accessed by the students. This will be where NETLAB+ administrators will spend most of their time adding pods, modifying pods, cloning pods, and deleting pods.

The best way to understand what is a pod is to simply view it as a personal lab environment for a student or team to use. Pods can be specifically made and assigned to students dependent on how the lab design is made for that particular pod or they can be made as a first come first serve pod for students who are associated with the class that uses the pod.

### 6.7.1 Adding Pods

Each pod is different, which makes creating each pod slightly different amongst the others. Depending on your requirements, be sure to visit the following page to see an updated list of available pods that can be made in NETLAB+. Towards the bottom of the page, select the proper pod documentation to view how that particular pod needs to be configured.

http://goo.gl/nAF5T1

### 6.7.2 Adding Custom Pods

NETLAB+ provides functionality by enabling users to create their own pod designs and lab designs. You have the option of using the general IT topologies which can be substituted for your own virtual machine guest operating systems. More information about the general IT topology can be found here: http://goo.gl/Z5dJ3a

If you wish to make an entire topology custom made, you may do so. NDG has documented two guides that can be used for guidance when attempting to make a new topology from scratch. More information about building your own NETLAB+ topology and labs can be found here: http://goo.gl/OJ7Abe

# 7 Lab Reservations

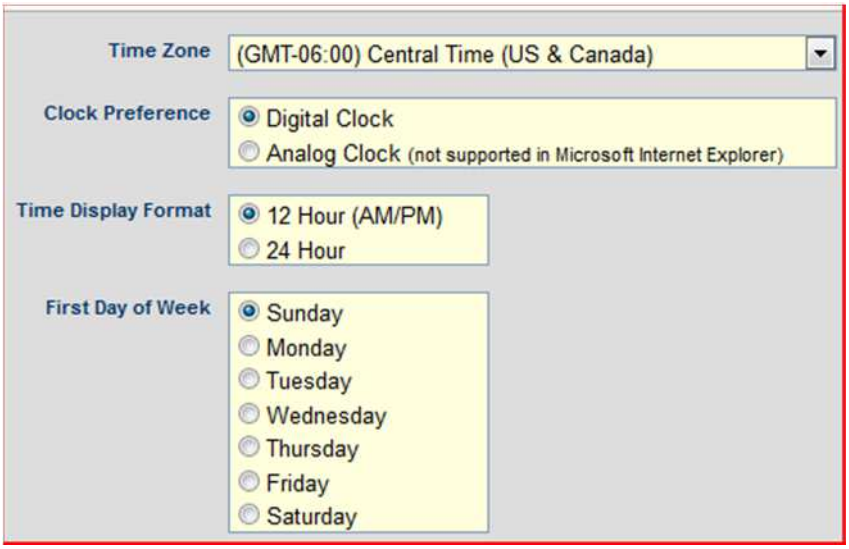
## 7.1 Scheduling a Lab Session as a Student

This section will demonstrate how to schedule a lab session as a student. Based on your NETLAB+ configuration, please give your students the proper URL to access the campus NETLAB+ system.

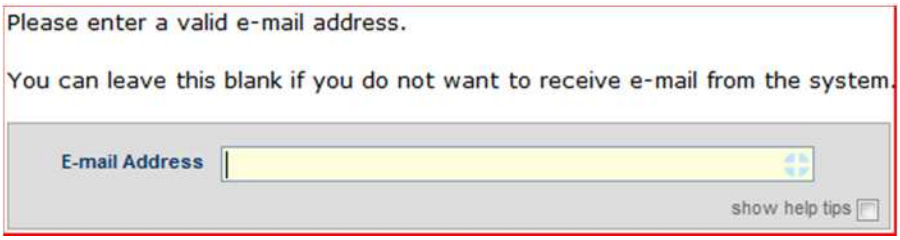
The following steps will help guide the process of making a reservation:

1. Enter the NETLAB+ URL address into a supported web browser.
2. Login using the username and password that has been provided by a NETLAB+ administrator.
3. Upon first login, you will be asked to enter a new password. Enter password and continue.

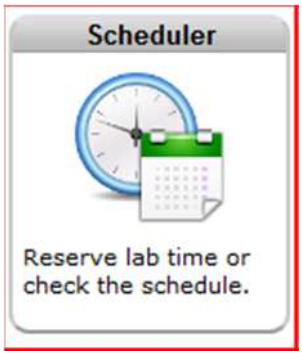
4. Select your time zone.



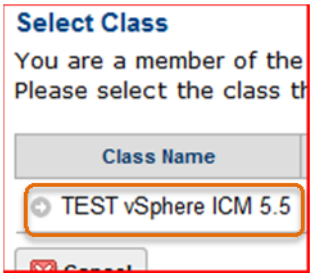
5. This part is optional, but you may enter an email address to receive NETLAB+ notifications.


Please enter a valid e-mail address.
You can leave this blank if you do not want to receive e-mail from the system.
E-mail Address
show help tips

6. Select the **Scheduler** icon.



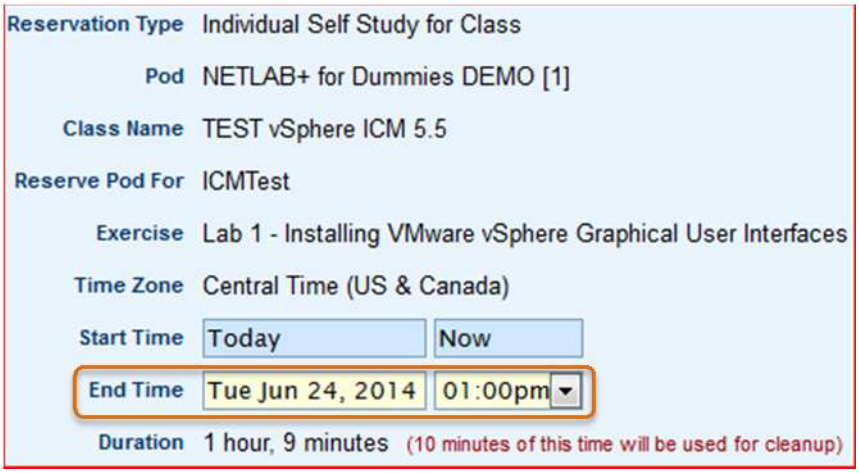

7. On the next page you will be prompted to select a class. The student will choose the appropriate class that they are enrolled in to complete their labs.



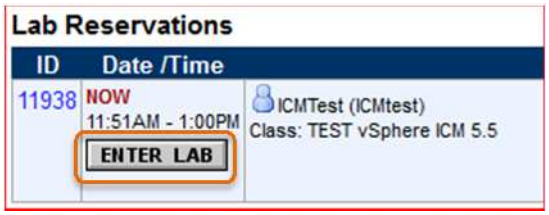

8. On the *Scheduling Options* page, the student will have the option to either choose lab time for themselves or lab time as a team (if available). Most of the time the student will select **Reserve lab time for yourself**.
9. The student will then select the appropriate exercise by choosing which lab to do. The exercises can be switched later when in the pod environment.
10. The student will then select an available time slot by clicking below any available pod next to a time slot that is convenient for the student. (Tip: Click directly below

the red line to schedule a pod beginning at the current time. It will show "NOW" as the start time.)

11. The student can adjust end time via the *End Time Dropdown* box.




12. Click on **OK** to continue.
13. Click on **I'm Done** to advance to your reservation.
14. In the *Lab Reservation* window, the session you created is now visible. You can click on the **Enter Lab** button to begin your lab. If the *Enter Lab* button is not visible, the reservation time slot has not been reached yet.



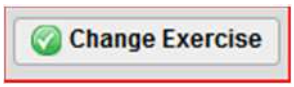

15. Once in the pod environment, you may view the lab instructions by clicking on the **Show Lab Content** button at the bottom of the *Topology* tab.

## 7.2 Changing Lab Exercises

The following steps will help guide through the process of changing lab exercises:

1. It is assumed that you already entered the active pod reservation. See steps in Section 7.1.
2. Click the **Exercise** tab at the top of the main interface window.

3. You can now select the next lab exercise and click **Change Exercise**.



# 8 Best Practices

## 8.1 Background

This part of the guide is labeled as “Best Practices” because it will highlight important configurations that will be used consistently by a NETLAB+ administrator.

## 8.2 Normal vs. Persistent VMs

There are two virtual machines roles that people tend to mix up at times. It is important to know the differences between a VM that has a “normal” role as opposed to a VM that has a “persistent” role. Both of these are available configurations when viewing VM details in NETLAB+.

### 8.2.1 Normal

A normal VM is assigned to a production pod that is configured to revert back to an available snapshot at the beginning and end of a lab reservation. When a user invokes the scrub action on the VM or entire pod, it will revert back to its snapshot as well.

Setting a virtual machine’s role to “normal” is an ideal choice for pods that should always start in the same state. The list below is a current list of lab designs that utilize the “normal” VM role:

- Cisco Pods
- Linux+ Base
- Linux+ Install
- CNSS 4011
- Multi-Purpose Security (MSEC)
- Ethical Hacking (EH)
- Forensics
- Network+
- VMware vSphere ICM 5.5
- A+

### 8.2.2 Persistent

A persistent VM is assigned to a production pod that is configured to retain the current state of the virtual machine from one reservation to the next. A persistent VM never reverts back to a snapshot. The practical use for this is when students need to be able to save their work done to a VM as the class continues on.

Settings a virtual machine's role to "persistent" is an ideal choice for pods that need to be able to carry results progressively for each lab assignment. The list below is a current list of lab designs that utilize the "persistent" VM role:

- EMC ISM
- VMware View ICM 5.1
- VMware vSphere ICM 5.1

## 8.3 Breakdown of Proper Pod Creation & Cloning

When first starting out as a NETLAB+ administrator, it can become unclear on what the proper procedure is to create equipment pods for your classes. This section of the guide will highlight what steps need to be taken by an administrator to create and add equipment pods in an efficient way.

*Note: This procedure assumes that you are using local ESXi disk storage (NDG recommended) and not a storage area network (SAN). Also, adding Cisco pods will not be covered as those require a different procedure to add.*

### 8.3.1 Importing VMs into the Virtual Machine Inventory

When beginning to create master pods, it is important to know that you first need to important the first set of virtual machines from your vCenter datacenter. When you download the zipped VM packages from CSSIA, you need to import them into vCenter as .ova files. Once you have the required master VMs in your vCenter, you may then proceed to import them into the NETLAB+ Virtual Machine Inventory.

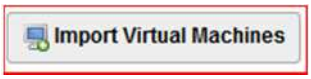
The following steps will help guide you through the process of importing VMs into the Virtual Machine Inventory.

1. Login to the NETLAB+ system using an administrator account.

2. Click on the **Virtual Machine Infrastructure** icon.

3. Click the **Virtual Machine Inventory**.

4. Click the **Import Virtual Machines** button at the bottom of the page.

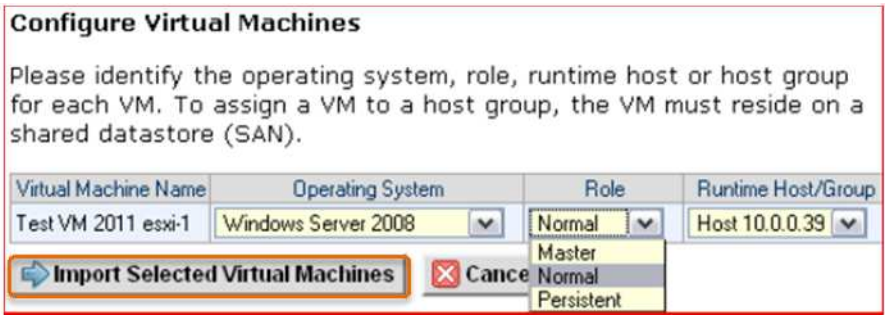



5. You will now be presented with the option of choosing which datacenter that is linked to the NETLAB+ system. Choose the appropriate datacenter by clicking on the name.
6. NETLAB+ will now scan the datacenter to discover any virtual machines that are not currently in the inventory.

7. Place a **check mark** in each box next to the virtual machine name that you wish to import and then click **Import Selected Virtual Machines**.

8. In most cases, we will be importing master VMs first and then cloning them later on, so be sure to select "**Master**" under the *Role* column.
9. Select the closest operating system that you are importing by selecting the appropriate type under the *Operating System* column.

10. After selecting the configuration settings and selecting **Import Virtual Machines**, the VMs will be added to the NETLAB+ inventory.


Configure Virtual Machines
Please identify the operating system, role, runtime host or host group for each VM. To assign a VM to a host group, the VM must reside on a shared datastore (SAN).
Virtual Machine Name
Operating System
Role
Runtime Host/Group
Test VM 2011 esxi-1
Windows Server 2008
Normal
Host 10.0.0.39
Master
Normal
Persistent
Import Selected Virtual Machines
Cance

Referenced from NETLAB+ Remote PC Guide Series - NetDevGroup.com

11. Select **OK** to return to the inventory.

### 8.3.2 Creating a Master Pod

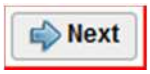
The first step when adding new equipment pods to NETLAB+ is to make sure you start out with a "Master Pod".

The following steps will help guide through the process of creating a master pod:

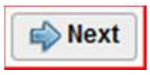
1. Create a new pod in NETLAB+ with the desired pod design by first logging into the NETLAB+ system using an administrator account.
2. Click on the **Equipment Pods** icon.

3. Towards the bottom, click on **Add a Pod**.

4. On the *New Pod Wizard*, click **Next** to continue.

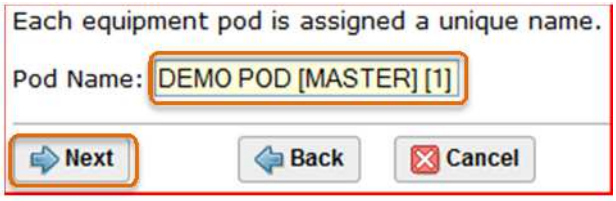



5. Here you will select the pod type that you'd like to create by filling in the bubble next to a desired pod type and then clicking on **Next** at the bottom.

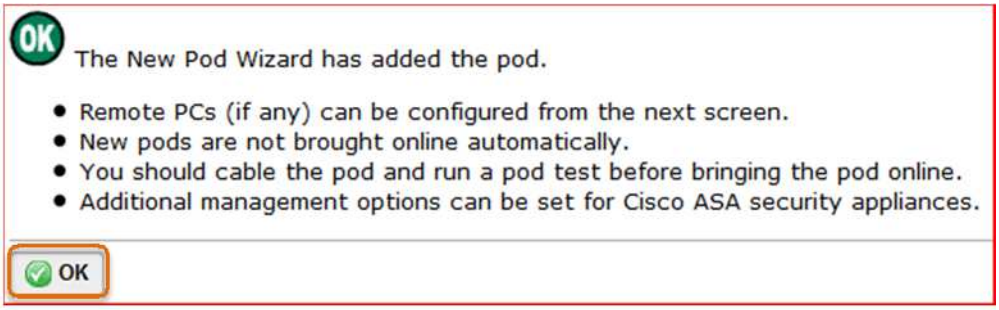



6. Select the **Pod ID** you wish to choose. This is more of an organizational unit that will depend on your organizational standards (it is a good practice to allocate pods 1000 – 1050 for master pods.). Click **Next**.

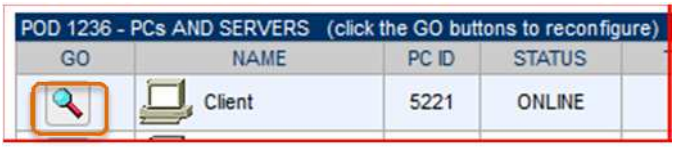
7. Enter a **Pod Name** in the field (It is a good idea to have a naming convention that includes **[MASTER]** for each master pods.). Click **Next** to continue.




8. Click **OK** to finish the pod creation.

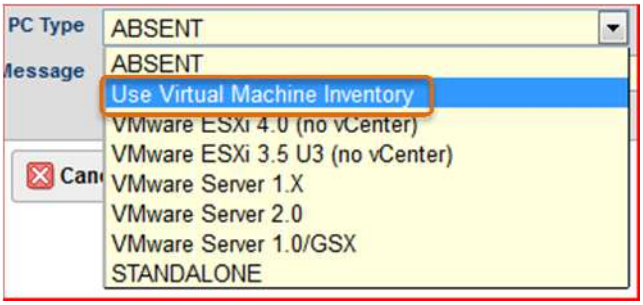

OK
The New Pod Wizard has added the pod.
Remote PCs (if any) can be configured from the next screen.
New pods are not brought online automatically.
You should cable the pod and run a pod test before bringing the pod online.
Additional management options can be set for Cisco ASA security appliances.
OK

9. Now you will be required to add VMs that will map to each remote PC position for the pod type you are targeting (you should have these VMs already downloaded from *CSSIA*.).
10. To add a VM, click on the "**magnifying glass**" next to the PC name.

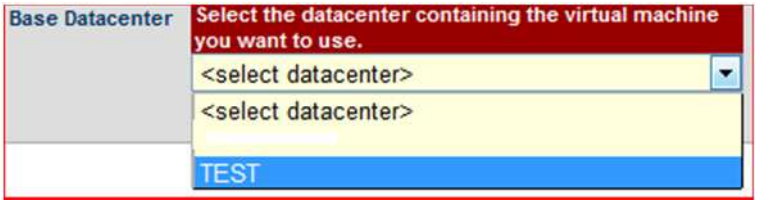



11. Click on **Modify PC Settings**.

12. Click on the drop-down box next to *PC Type* and select *Virtual Machine Inventory* (you should already have VMs loaded into your *Virtual Machine Inventory* from Section 8.3.1.).




13. Choose the *Base Datacenter* to the datacenter that is managing your specified VMs.



14. Now you will receive another option, "*Base Virtual Machine*". Here you will select the virtual machine by name.

15. Once selected, the VM will be added to the pod.
16. Repeat steps 10 through 15 to add the remaining VMs.
    a. Double-check to make sure that each virtual machine in the master pod has its role set to **master**. Again, this can be accomplished by clicking on the **magnifying glass** next to the VM name when viewing the pod details.

17. Add snapshots while the virtual machines are powered down. You can do this from the NETLAB+ action tab or from the *vSphere Client* (It is recommended to use a naming convention that follows "**GOLDEN_MASTER**").

> *If you have more than one ESXi Host Server, it is advised to space out your VMs evenly between each host. If this path is used, make sure to do a "full clone" of your master pods to the other ESXi Host Server. (This all depends on your topology, however, it is best practice to load balance between two hosts at minimum.)*

18. Once each virtual machine in the master pod has a golden snapshot, linked clones are possible.

### 8.3.3 Link Cloning a Master Pod

Once the Master Pods are in place, you may proceed with cloning each master pod to produce a production pod that will be used by the students.

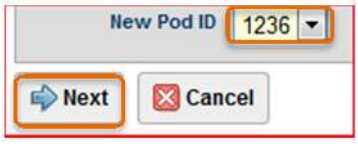
The following steps will help guide through the process of link cloning:

1. Login to the NETLAB+ system using an administrator account.
2. Click on the **Equipment Pods** icon.

3. Select the **Master Pod** you wish to clone. Remember, you may do so by either clicking on the **magnifying glass** or **pod ID**.
4. Begin the clone process by clicking the **Clone** button.

Test
Tell me if this pod is working properly.
Clone
Create a new pod based on the settings of this pod.
Rename
Rename this pod.

5. Select a **New Pod ID** for the new pod and click **Next**.




6. Specify a **unique descriptive name** for the new pod (it is a good practice to assign even numbers after the pod name to represent one ESXi Host Server and odd numbers to represent another ESXi host that will be used to host the pods that are about to be cloned. Again, this brings back the concept of load balancing between two or more hosts.) Click **Next** to continue.

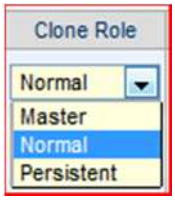
7. Verify that each source virtual machine is set to the correct master virtual machine.

8.

9. Verify that each source snapshot is set to the golden snapshot.

10. Set each clone type to **Linked**.

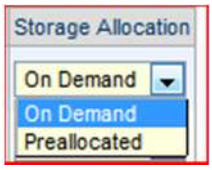
11. Set the role to either **Normal** or **Persistent**, depending on what pod type you are creating (Refer to Section 8.2).




12. Verify that the *Runtime Host* is the ESXi server where each VM will run on. This should be set to the same host containing the master VMs unless your VMs are located on a SAN. (Again, this is why we did a full clone of the master pod on each server. You will click on the other master pod to clone from and will notice that the *Runtime Host* will be different when attempting to link clone.)

13. Set the *Clone Datastore* to a datastore accessible by the *Runtime Host*.

14. Verify that the *Storage Allocation* setting is set to **On Demand**.




15. Once the necessary configurations are in place, click **Clone Pod** to start cloning.

16. Repeat steps 3 through 14 to clone additional production pods until desired count is reached.

# 9 References

Al information and documentation can be found by visiting http://netdevgroup.com.

**NETLAB+ Remote PC Guide Series**

- Remote PC Guide Series Directory: http://goo.gl/xwhPWt

**General System Documentation for NETLAB+**

- NETLAB+ System Overview: http://goo.gl/672udl
- NETLAB+ Installation Guide: http://goo.gl/HmFytM
- NETLAB+ Administrator Guide: http://goo.gl/l8bhSQ
- NETLAB+ Instructor Guide: http://goo.gl/L0i8B7
- NETLAB+ Student Guide: http://goo.gl/aj8V5u
- NETLAB+ Pod Assignment Guide: http://goo.gl/HeAnJd
- NETLAB+ Pod Design Guide: http://goo.gl/dEQRZD
- NETLAB+ Lab Design Guide: http://goo.gl/xB5ZP4
- NETLAB+ Product Summary: http://goo.gl/t8i2Hh

**VMware Licensing Guidance**

- VMAP vs. vITA Chart: http://goo.gl/iza4I0

**Requesting Preconfigured VMs from CSSIA**

- CSSIA Preconfigured Virtual Machine Requests: http://goo.gl/Bm5xnu

**Connectivity and Firewall Suggestions**

- CSS, Connectivity and Firewall: http://goo.gl/fjsBCK

**Frequently Asked Questions**

- FAQs: http://goo.gl/ni5N3B